(19) KOREAN INTELLECTUAL PROPERTY OFFICE

KOREAN PATENT ABSTRACTS

(11)Publication number: 100400947 B1
(43)Date of publication of application: 25.09.2003

(21)Application number: 1020020073773
(22)Date of filing: 26.11.2002

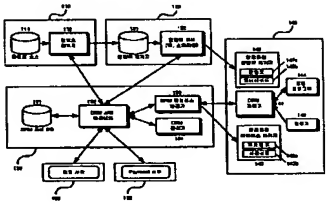
(71)Applicant: CORETRUST INC.
(72)Inventor: WOO, JE HAK
LEE, HWAN CHUL
CHO, SANG YOUNG
JEONG, SEONG HO
HA, YOUNG SOO
SHIN, SEOG KYOON

(51)Int. Cl G06F 17/00

(54) SYSTEM AND METHOD FOR PROTECTING INFORMATION OF MULTIMEDIA STREAMING CONTENTS, AND RECORDING MEDIUM RECORDING THE SAME

(57) Abstract:

PURPOSE: A system and a method for protecting information of multimedia streaming contents, and a recording medium recording the same are provided to safely protect a copyright without increasing a server or occurring network traffics while using a multimedia file format or a protocol of a current streaming scheme.



CONSTITUTION: An information providing system includes an encryption tool(110) generating a contents package(121) by encrypting a contents source(111), a providing tool(120) providing the encrypted contents package to a user, and a DRM(Digital Rights Management) server(130) generating/managing an encryption key and performing various certifications. A client system(140) includes a controller activating an application program and controlling a filtering tool, and the application program(144) receiving/playing the encrypted contents from the filtering tool. The data received by the filtering tool is received through a network driver connecting to an external network, and the multimedia streaming contents are a live/VOD(Video On Demand) method.

Legal Status
Date of final disposal of an application (20030826)
Patent registration number (1004009470000)
Date of registration (20030925)

(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.[7]
G06F 17/00

(45) 공고일자 2003년10월08일
(11) 등록번호 10-0400947
(24) 등록일자 2003년09월25일

(21) 출원번호 10-2002-0073773
(22) 출원일자 2002년11월26일
(65) 공개번호 특0000-0000000
(43) 공개일자 0000년00월00일

(73) 특허권자 주식회사 코어트러스트
서울 강남구 역삼동 769-7 동아빌딩 6층 2호

(72) 발명자 우제학
서울특별시 성동구 금호동4가 800번지 대우아파트 108-902

이환철
인천광역시 연수구 동춘2동 932 26/4한양2차아파트 35동 311호

조상영
경기도 용인시 모현면 왕산리 464-2 풍산아파트 104-1504

정성호
경기도파주시아동동팜스프링아파트126동1202호

하영수
서울특별시노원구공릉2동408-1303층

신석균
서울특별시강북구미아동벽산라이브파크아파트103-503

(74) 대리인 홍재일

심사관 : 송대종

(54) 멀티미디어 스트리밍 콘텐트의 정보보호 시스템과 방법 및이를 기록한 기록매체

요약

본 발명은 유무선 인터넷을 통한 스트리밍 방식으로 제공되는 동영상, 영화, 음악, 온라인 교육콘텐트 등의 디지털 콘텐트를 불법복제 및 불법전송하는 것과 같은 저작권 침해행위를 원천적으로 차단할 수 있는 정보보호 방법 및 시스템에 관한 것이다.
본 발명의 목적은 커널 모드에서의 제어기술을 이용하여 스트리밍 방식으로 제공되는 다양한 콘텐트 및 다양한 단말기, 플랫폼을 지원함으로써 콘텐트의 최종 사용자에게는 편리함을, 저작권자에게는 수익을 동시에 보장할 수 있는 기술적인 방법을 제공하려는 것이다.
구체적으로는 기존의 디지털 콘텐트의 정보보호 시스템은 암호화된 콘텐트를 보기 위해 복호화 수단을 가진 전용 뷰어 프로그램을 사용해야만 했으나, 본 발명에서는 네트워크 필터 드라이버를 제작함으로써 기존의 응용프로그램을 사용하여 콘텐트를 이용할 수 있도록 하였다. 또한 하나의 디지털저작권관리(DRM) 플랫폼을 사용하여 다양한 콘텐트 포맷과 다양한 서비스 방식을 동시에 지원할 수 있는 방법을 제공하고 있다. 또한 본 발명은 스트리밍 방식으로 전달되는 암호화된 멀티미디어 콘텐트 데이터에 대하여 네트워크 필터 드라이버를 이용하여 메시지와 패킷의 후킹 및 변경, 암호화된 데이터의 복호화, 응용프로그램으로 전달하는 필터링 방법을 제공하고 있다. 또한 본 발명은 라이브 및 VOD 스트리밍 방식으로 제공되는 콘텐트를 효율적으로 암호화 및 복호화하는 방법을 제공하며, 커널 모드에서 보

안요소를 만들어 줌으로써 보안수준을 한층 높여주는 방법을 제공한다.

대표도

도 6

색인어

콘텐트, 커널 모드, 스트리밍, 정보보호, 디지털저작권관리, Digital Rights Management, DRM, 네트워크 필터 드라이버

명세서

도면의 간단한 설명

도 1은 본 발명의 디지털저작권관리(DRM) 시스템의 전체 모식도.
도 2는 콘텐트 제공 시스템에서의 암호화된 콘텐트 패키지의 생성과정을 보여주는 모식도.
도 3은 사용자가 스트리밍 방식으로 암호화된 멀티미디어 콘텐트를 플레이하는 과정을 보여주는 모식도.
도 4는 클라이언트 시스템에서의 스트리밍 콘텐트를 플레이하는 과정의 모식도.
도 5는 네트워크의 계층구조에서 네트워크 필터 드라이버의 위치에 관한 모식도.
도 6은 암호화된 스트리밍 콘텐트 데이터의 이동과정을 보여주는 모식도.
도 7은 응용 프로그램이 네트워크 연결을 이루기 위한 준비과정을 보여주는 흐름도.
도 8은 응용 프로그램이 네트워크 연결을 이루는 과정을 보여주는 흐름도.
도 9는 스트리밍 방식으로 수신한 데이터의 복호화 과정을 보여주는 흐름도.
도 10은 멀티미디어 스트리밍 콘텐트의 파일 형식을 보여주는 모식도.
도 11은 DRM 패키지의 헤더 형식을 보여주는 모식도.
도 12A는 마이크로소프트의 윈도우 운영체제를 보여주는 모식도
도 12B는 마이크로소프트의 WinCE 운영체제를 보여주는 모식도
도 12C는 리눅스 운영체제를 보여주는 모식도
도 12D는 팜(Palm) 운영체제를 보여주는 모식도
도 12E는 일반 휴대폰의 운영체제를 보여주는 모식도
도 13은 본 발명에서 암호화를 수행하는 콘텐트 패키저 프로그램의 화면 이미지
도 14는 본 발명에서 DRM 관리기 프로그램의 화면 이미지
도 15는 본 발명에서 암호화된 VOD 스트리밍 콘텐트를 복호화하여 기존의 응용 프로그램으로 보여주는 화면캡처의 이미지
도 16은 본 발명에서 암호화된 VOD 스트리밍 콘텐트를 복호화하여 OCX 플레이어로 보여주는 화면캡처의 이미지
도 17은 본 발명에서 암호화된 라이브 스트리밍 콘텐트를 복호화하여 OCX 플레이어로 보여주는 화면캡처의 이미지
도 18은 본 발명에서 복호화되지 않은 콘텐트를 플레이할 때 화면캡처의 이미지
<도면의 주요부분에 대한 설명>
112: 콘텐트 패키저 122: 콘텐트 서버
130: DRM 서버 132: DRM 서버 콤포넌트
141: DRM 제어기 403: 네트워크 드라이버
404: 네트워크 필터 드라이버 506: TDI 드라이버

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명의 목적은 유무선 인터넷을 통하여 스트리밍 방식으로 제공되는 멀티미디어 콘텐트의 정보보호 시스템과 방법 및 이를 기록한 기록매체에 관한 것으로서, 좀 더 상세하게는 동영상 및 영화, 음악, 온라인교육 등의 멀티미디어 콘텐트를 스트리밍 방식으로 서비스할 때, 네트워크 트래픽 또는 서버의 과부하 없이 콘텐트를 암호화하여 배포하고 정당한 사용권한을 획득한 사용자에게만 복호화할 수 있도록 지원함으로써, 불법복제 및 불법전송 등의 저작권 침해

행위를 원천적으로 차단하고, 전용뷰어 프로그램을 사용하지 않고 기존의 응용프로그램을 사용해서 콘텐트를 볼 수 있으며, 또한 네트워크 필터 드라이버 단계에서 메시지와 패킷의 후킹(hooking, 가로채기) 및 변경, 복호화, 전달의 필터링 작업을 수행함으로써 한층 보안성능을 높인 라이브 및 VOD(Video On Demand) 스트리밍으로 제공되는 멀티미디어 콘텐트의 정보보호 시스템과 방법 및 이를 기록한 프로그램 기록매체를 제공하는 것이다.

최근 컴퓨터와 인터넷, 저장매체 등의 급속한 발전에 따라 각종 문서와 콘텐트 등이 컴퓨터가 읽을 수 있는 디지털 데이터 형태로 제작되어 유통되고 있다. 그러나, 이러한 디지털 콘텐트는 특성상 원본과 동일한 복사본 또는 변형본을 쉽게 만들어 낼 수 있을 뿐만 아니라 손쉽게 배포할 수 있다는 치명적인 문제점이 있다. 따라서 많은 자금과 시간, 창의력, 노동력이 들어가는 디지털 콘텐트의 저작자 입장에서는 자신의 저작권을 온라인 또는 오프라인에서 철저히 보호하기를 원하지만, 이는 쉬 운 일이 아니며, 결국 상술한 바와 같은 디지털 콘텐트의 불법복제와 불법배포의 위험성은 디지털 콘텐트 산업의 활성화에 큰 장애가 되고 있다.

이러한 디지털 콘텐트의 저작권을 보호하기 위해서 최근 관심이 고조되고 있는 것이 디지털 저작권 관리(Digital Rights Management, 이하 'DRM'이라 함) 시스템이다. DRM 시스템이란 다양한 채널을 통해 유통되는 텍스트, 음악, 이미지, 영상, 동영상강의, 영화, 소프트웨어, 게임 등 각종 디지털 콘텐트를 불법복제로부터 보호하면서 지속적인 콘텐트 유료화 서비스를 가능하게 하는 기술이다. 최근 MP3 음악파일 교환 사이트인 미국의 냅스터와 우리나라의 소리바다 사이트, 또한 영화의 불법유통 사이트에 대한 저작권 분쟁이 첨예한 사회문제로 대두되고 있으며, 이와 같은 저작권 침해 논란을 근본적으로 해결해 줄 수 있는 가장 확실하고 유일한 방안으로서 DRM 시스템에 대한 많은 기술개발 및 제품화가 진행되고 있다.

이러한 DRM 시스템을 도입하면 콘텐트를 미리 암호화하므로 공급자가 정한 규칙과 사용정책을 충족할 경우에만 그 콘텐트를 사용자가 열어볼 수 있으며, 설령 불법복제가 되더라도 콘텐트가 암호화되어 있기 때문에 정당한 비용을 지불하지 않은 사용자는 열어 볼 수가 없게 된다. 또한, DRM은 단순히 저작권을 보호하는 것 뿐만 아니라, 콘텐트 사용자간의 슈퍼배포(superdistribution)와 같은 새로운 콘텐트 판매 및 유통 기술로서도 잠재적 가치를 가지고 있다.

여기서, 넓은 의미의 디지털 저작권에 대한 관리 기술은 방금 상술한 DRM 기술 이외에도 PKI(Public Key Infrastructure, 공개키) 기반의 불법복제 방지기술, DOI(Digital Object Identifier, 디지털 콘텐트 식별체계) 기반 저작권 보호 기술, 워터마킹(watermarking) 기술 등을 모두 포함하고 있지만, 현재 세계적으로 가장 큰 기대를 모으고 있는 것은 역시 DRM 기술이다.

또한, 디지털 저작권에 대한 관리 기술을 저작권 보호 시점을 기준으로 분류하면, DRM 기술과 같이 콘텐트의 유통 및 배포단계 이전에 미리 암호화하는 사전(事前)적 저작권 보호 기술과, 워터마킹과 같이 유통 및 배포단계 이후의 디지털 콘텐트 저작권 보호를 목적으로 하는 사후(事後)적 저작권 보호 기술로 나눌 수 있다.

또한, 응용분야별로 분류하면, 유선 인터넷을 위한 DRM, 휴대폰과 PDA를 위한 무선 DRM(mobile DRM), 홈 VOD를 위한 셋톱박스(set-top box) DRM 등으로 나눌 수 있다.

또한, 적용 대상 콘텐트의 유형을 기준으로 분류하면 문서보안 DRM과 멀티미디어 콘텐트 보안 DRM으로 나눌 수 있으며, 특히 멀티미디어 콘텐트 보안 DRM은 기술적인 난이도에 따라 다운로드 방식만 지원하느냐, 아니면 VOD 및 Live 스트리밍까지도 지원하느냐로 구분할 수 있다.

현재 이러한 DRM 관련업체로는 1990년에 세계적으로 가장 빨리 DRM 기술개발을 시작한 인터트러스트(www.intertrust.com)를 비롯하여 마이크로소프트(www.micorsoft.com), IBM, 콘텐트가드(www.contentguard.com), 리얼네트웍스(www.realnetworks.com), 록스트림(www.lockstream.com), 디지막(www.digimarc.com), 디빅스네트웍스(www.divxnetworks.com), 엔트릭(www.entriq.com), 실드미디어(www.sealedmedia.com), 소니(www.sony.com), NEC(www.nec.com) 등이 있다. 또한, 국내에도 약 30개 이상의 DRM 관련 벤처기업들이 있으며, 대표적으로 본원발명의 출원인인 코어트러스트(www.coretrust.com)를 비롯하여 마크애니(www.markany.com), 파수닷컴(www.fasoo.com), 실트로닉테크놀로지(www.sealtronic.com), 디지캡(www.digicaps.com), 테르텐(www.teruten.com), 아르파(www.arpasec.com), 드림인테크(www.dreamintech.com) 등이 치열한 기술개발 및 상용화 경쟁을 벌이고 있다.

그러나 이러한 필요성에도 불구하고, 일반적인 예상과는 달리 전 세계적으로 DRM 관련시장의 형성은 매우 느리게 진행되고 있으며, 그 이유는 지금까지 출시된 대부분의 DRM 시스템들이 기술적 취약성을 가지고 있었기 때문이라고 분석되고 있다.

예를 들어, 지금까지의 대부분의 DRM 시스템들은 최종 사용자에게 전용 뷰어 프로그램의 설치를 강요하는 불편함이 있었으며, 또한 지원하는 콘텐트의 종류에도 많은 제한이 있었고, 뿐만 아니라 다양한 단말기 환경에 따른 호환성의 부족 등의 심각한 문제점을 근본적으로 해결해 주지 못하고 있었다. 특히 종래의 전용 뷰어 프로그램을 사용하는 DRM 시스템은 사용자에게 DRM을 적용한 콘텐트라는 거부감을 가지게 하였고, 하나의 전용 뷰어 프로그램에서 지원하는 콘텐트 파일 포맷에는 제한이 있을 수 밖에 없었으므로 서비스를 제공하고자 하는 수많은 파일 포맷과 응용 프로그램에 대응하는 각각의 전용 뷰어 프로그램을 제작해야만 하였으며, 또한 이 전용 뷰어 프로그램에 대한 지속적인 업그레이드를 시켜 주어야 한다는 단점이 있었다.

게다가, 지금까지 개발된 대부분의 멀티미디어보안 DRM 시스템은 클라이언트 단말 기에 다운로드된 상태에서만 볼 수 있도록 한정되어 있는 실정이다. 물론, 세계적으로 VOD 스트리밍을 지원하는 DRM 기술을 확보한 회사도 있지만, 마이크로소프트와 리얼네트웍스 등 3-4개 업체에 한정되어 있으며, 특히 라이브 스트리밍(live streaming)을 지원하는 DRM 제품은 아직 개발되지 못하고 있는 실정이다.

이 중에서 마이크로소프트는 아직까지 본격적인 DRM 시장이 형성되지 않았다고 판단하기 때문에 DRM SDK(Software Development Kit)의 라이센스를 무료로 배포하면서 시장 지배력을 키우고 있는데, 이 마이크로소프트 DRM 기술의 최대 약점은 오직 마이크로소프트 파일 포맷에만 한정하여 DRM을 적용할 수 있다는 점이다.

불법복제를 막고 대용량의 멀티미디어 콘텐트를 서비스하기 위하여 일반적으로 많이 사용되고 있는 스트리밍(streaming) 기술은 일반적인 웹 서비스를 통한 데이터의 전달처럼 콘텐트를 모두 서버로부터 클라이언트로 다운로드하여 그것을 다시 화면에 디스플레이하는 형태의 기술이 아니라, 다운로드와 플레이를 동시에 할 수 있도록 함으로써 다운로드되는 동안 기다려야 하는 불편함을 제거한 특별한 데이터 전송 기술이다. 이러한 스트리밍을 통하여 수신받은 데이터는 클라이언트의 하드디스크에 저장되는 것이 아니라 램 메모리 상에서만 일시적으로 저장 및 사용이 가능하도록 되어 있다. 대표적으로 스트리밍 기술은 미리 멀티미디어 콘텐트를 제작해 서버에 올려놓고 사용자의 요구에 따라 서비스하는 주문형 VOD 스트리밍과, 스포츠와 뉴스, 공연 등의 실시간 중계를 위한 라이브 스트리밍으로 나눌 수 있다.

그러나 2001년 7월에 훈넷(www.hoonnet.co.kr)이 개발한 하이넷 레코더(Hi Net Recorder)라는 프로그램은 스트리밍 방식으로 서비스되는 영화, 인터넷방송, 음악, 동영상강의, 뮤직비디오 등을 스트리밍으로 시청함과 동시에 자신의 컴퓨터에 저장할 수 있음을 보여줌으로써, 스트리밍 방식으로 서비스되는 디지털 콘텐트가 불법복제에 매우 취약하다는 것을 확인시켜 주었다.

일반적으로 클라이언트 시스템으로 사용되는 사용자 컴퓨터(Personal Computer, 이하 'PC'라 함), 노트북, PDA(Personal Digital Assistants), 휴대폰, 셋톱박스, 디지털TV, 텔레메틱스 단말기 등의 정보처리기기는 CPU, 메모리와 같은 휘발성 저장장치, 하드디스크와 같은 비휘발성 저장장치, 키보드와 모니터, 프린터와 같은 입출력장치, 유무선 내부 통신수단이나 외부 네트워크와의 통신수단과 같은 디바이스들을 가지고 있다. 이와 같은 정보처리기기들은 각각의 하드웨어와 소프트웨어로 구성되어 있으며, 특히 디바이스 드라이버는 실제 디바이스를 구동하는 소프트웨어로서, 실제 디바이스를 응용 프로그램에 연결시켜 주는 역할을 담당하고 있다.

상기 정보처리기기에는 다양한 디바이스 드라이버들이 계층구조를 이루고 있으며, 이러한 디바이스 드라이버의 계층구조에 특정한 역할과 기능을 수행할 수 있는 필터 드라이버를 임의로 제작하여 기존의 디바이스 드라이버 계층구조 내에 필터처럼 적절하게 삽입할 수 있다. 대표적인 디바이스 드라이버로서 하드디스크와 같은 저장장치를 제어하면서 파일과 디렉토리들을 관리하는 파일시스템 드라이버와, 외부 네트워크와의 통신을 담당하는 네트워크 장치를 관리하는 네트워크 드라이버를 들 수 있다. 이외에도 각각 가상메모리, CPU, 프로세스 관리, 멀티태스킹, 프린터, 키보드, 모니터 등을 관리하는 디바이스 드라이버들이 있다.

최근에 DRM 시스템을 적용할 때 전용 뷰어 프로그램의 단점을 해소하려는 기술로 서 제안된 것 중에 (주)테르텐이 출원한 '디지털 데이터의 안전한 전달 및 실행을 위한 보안 시스템(한국특허출원 10-2001-0034583)'이 있다. 상기 기술은 저장장치에 특정저장영역을 별도로 생성하고, 특정 실행 프로그램만이 상기 특정저장영역에 접근할 수 있도록 필터단을 제어하는 필터단 제어기와, 상기 특정저장영역 내의 모든 데이터의 입출력을 제어하면서 등록된 실행프로그램의 데이터 호출만을 유효한 것으로 판정하여 실행하도록 하는 파일시스템 필터단으로 구성되어 있다.

그러나 상기 기술은 필터단을 통해 응용프로그램을 제어하는 일반적인 기술을 포괄적으로 기술한 것에 불과하며, 저장장치 내에 별도 관리를 하는 특정저장영역의 부가적 설치가 필요하고, 암호화가 풀린 콘텐트 데이터 파일을 상기 특정저장영역에 보관함으로써 보안상의 허점이 발생할 수 있으며, 응용 프로그램을 파일시스템 필터단에 모두 등록 및 관리하여야 하는 불편함이 있고, 암호화 및 복호화에 대한 구체적인 언급이 거의 되어있지 않다. 그리고 발명의 주요 목적이 특정 개발사의 DRM 제어기에 구애받지 않는 정보보호 시스템을 제안하는 것이라는 한계가 있다.

또한 (주)테르텐이 상기 특허와 관련하여 추가적으로 출원한 기술로서 '스트림 방식으로 실행되는 디지털 데이터의 보호를 위한 시스템 및 방법(한국특허출원 10-2001-0050151)'이 있다.

그러나 그 제목에는 "스트림 방식"으로 실행되는 디지털 데이터의 보호를 위한 시스템으로 표현되어 있으나, 그 내용을 분석해 보면 실제로는 일반적인 의미에서의 스트리밍 콘텐트의 서비스에 적용할 수 있는 DRM 기술이 아님을 쉽게 알 수 있다. 왜냐하면 상기 기술은 클라이언트 시스템에 다운로드 받은 파일을 파일시스템 내의 "내부 스트림 공급 수단"을 이용하여 응용 프로그램에 전달하는 방식을 취하고 있고, 또한 파일시스템 필터 드라이버를 이용하여 구현한 정보보호 기술이기 때문이다. 따라서, 일반적인 스트리밍 콘텐트의 서비스에 적용할 수 없는 한계를 가지고 있다.

한편, 이러한 파일 시스템 필터 드라이버를 이용한 데이터보안에 대한 매우 자세하고 광범위한 기술로서 미국의 인프라워크스사가 출원한 '데이터보안 제공을 위한 시스템과 방법'(한국특허출원 10-2001-7006901)이 있다.

그러나 상기 기술도 주로 하드디스크와 같은 저장장치의 입출력을 관리하는 파일시스템 필터 드라이버를 이용하는 패키저와 리시버로 구성된 것으로서, 엄밀한 의미에서 하드디스크와 같은 저장장치를 사용하지 않고 단지 램 메모리에서만 데이터의 일시적인 저장 및 사용을 지원하는 스트리밍 방식의 멀티미디어 콘텐트의 정보보호에는 적용되지 못하는 한계를 가지고 있다.

이들 종래기술과 별도로, 본원 발명의 출원인인 (주)코어트러스트는 2002년 1월 12일에 출원한 기술인 '디지털 콘텐트의 정보보호 방법 및 시스템'(한국특허출원 10-2002-0001916)에서는 파일 필터 드라이버를 이용하여 기존의 응용 프로그램을 제어함으로써, 다운로드 방식과 HTTP 스트리밍 방식을 지원하는 DRM 시스템에 대해 획기적이고 상세한 기술적 내용을 제시한 바 있다.

발명이 이루고자 하는 기술적 과제

본 발명은 상기 종래의 기술에서 암호화된 멀티미디어 콘텐트 데이터의 라이브 및 VOD 스트리밍 서비스를 지원하지 못했던 문제점을 완벽하게 해결할 수 있는 구체적 인 기술을 제공하려는 것이다.

즉, 본 발명의 목적은 스트리밍 방식으로 전달되는 멀티미디어 콘텐트의 불법복제의 문제점을 근본적으로 해결할 수 있는 디지털 콘텐트의 정보보호 방법 및 시스템, 프로그램 기록매체를 제공하는 것이다.

본 발명의 또 다른 목적은 기존의 스트리밍 방식의 멀티미디어 파일 포맷이나 프로토콜을 그대로 사용하면서 별도의 서버 증설이나 네트워크 트래픽의 발생없이 안전하게 저작권을 보호하는 방법을 제안하는 것이다.
본 발명의 또 다른 목적은 클라이언트 시스템에서 스트리밍 방식의 데이터를 수신하는 네트워크 드라이버단에서 작동하는 네트워크 필터 드라이버를 제작함으로써, 기존의 뷰어 및 플레이어 프로그램을 제어하여 전용 뷰어 프로그램을 사용하지 않고 다양한 파일 포맷을 손쉽게 지원할 수 있는 스트리밍 지원 DRM 시스템을 제안하는 것이다.
본 발명의 또 다른 목적은 네트워크 필터 드라이버가 응용 프로그램과 네트워크 드라이버 사이의 메시지와 패킷의 후킹 및 변경, 복호화, 전달하는 필터링 기능을 구비함으로써 스트리밍 방식으로 전달되는 암호화된 콘텐트 데이터의 원활한 복호화 및 안전한 저작권 보호 방법을 제시하는 것이다.
본 발명의 또 다른 목적은 암호화된 콘텐트 패키지를 만드는 콘텐트 제공 시스템이 기존에 지원할 수 없었던 라이브 스트리밍을 지원하는 방법을 제시하고, 또한 효율적으로 암호화 및 복호화하는 방법을 구체적인 방법을 제시하는 것이다.

발명의 구성 및 작용

상기와 같은 기술적 과제를 달성하기 위하여, 본 발명에서는 스트리밍 방식으로 서비스되는 멀티미디어 콘텐트에 DRM을 적용하기 위해서 클라이언트 시스템의 네트워크 필터 드라이버의 제작기술을 이용하여 응용 프로그램과 외부의 스트리밍 서버가 통신하는 메시지와 데이터 패킷의 후킹 및 변경, 복호화, 전달하는 필터링 수단의 구체적인 기술적 사상과 시스템, 방법 및 이를 기록한 기록매체를 제안한다.
보다 구체적으로는 본 발명에 의한 멀티미디어 스트리밍 콘텐트의 정보보호 시스템은
각각 CPU, 휘발성 저장장치(메모리), 비휘발성 저장장치(하드디스크), 입출력장치(키보드, 모니터 등)를 가지며, 유무선 내부 통신수단이나 외부 네트워크와의 통신수단에 의하여 연결되어 있는 정보제공 시스템과 클라이언트 시스템을 이용하여 스트리밍되는 멀티미디어 콘텐트의 정보를 보호하는 시스템에 있어서,
상기 정보제공 시스템은
콘텐트 소스를 암호화하여 콘텐트 패키지(121)를 생성하는 암호화 수단(110)과;
상기 암호화된 콘텐트 패키지(121)를 사용자에게 제공하는 공급 수단(120)과;
암호화키의 생성 관리와 각종 인증을 수행하는 DRM 서버(130);
으로 구성되며,
상기 클라이언트 시스템은
응용프로그램과 하위 레이어의 드라이버 사이에 위치하여 이들 간의 메시지와 패킷을 가로채고, 변경하고, 암호화된 데이터를 복호화하여 상기 응용프로그램에 전달하는 필터링 수단과;
응용프로그램을 활성화시키고, 상기 필터링 수단을 제어하는 제어수단과;
상기 필터링 수단으로부터 복호화된 콘텐트를 전달받아서 플레이하는 응용프로그램(144)과;
로 구성됨을 특징으로 한다.
여기서, 정보제공 시스템의 일 실시예에 의하면, 상기 암호화 수단(110)은 상기 DRM 서버(130)에서 생성시킨 암호화키를 전달받아 콘텐트의 암호화를 수행하는 콘텐트 패키저(112)일 수 있고, 상기 공급 수단(120)은 상기 암호화 수단(110)에 의하여 암호화된 콘텐트 패키지(121)가 업로드되는 콘텐트 서버(122)일 수 있다.
또한, 일 실시예에 의하면, 상기 DRM 서버(130)는
DRM 서버의 각종 콘텐트 정보, 암호화키, 사용자 정보, 응용 프로그램 정보 등을 저장하는 DRM 서버 DB(131)와;
DRM 암호화키의 발생 관리 및 라이센스 발급 관리를 제어하는 DRM 서버 콤포넌트(132)와;
클라이언트 시스템의 DRM 제어기(141)의 요청에 따라 암호화된 라이센스 패키지를 발급하는 DRM 라이센스 발급기(133)와;
DRM 서버의 설정과 관리를 수행하는 DRM 관리기(134);
로 구성될 수 있다.
또한, 일 실시예에 의하면, 상기 정보제공 시스템은 유료 서비스시의 비용청구를 위하여 빌링 서버(150) 또는 페이먼트 게이트웨이 서버(160)와의 연계 수단을 더욱 구비할 수 있다.
한편, 클라이언트 시스템의 일 실시예에 의하면, 상기 필터링 수단은 상기 제어수단의 지시에 따라 응용프로그램(144)과 외부의 공급 수단(120) 사이의 메시지와 패킷의 후킹 및 변경, 암호화된 콘텐트 패키지(142)의 복호화를 수행하여 상기 응용프로그램(144)에 전달하는 필터링 작업을 커널 모드에서 작동하는 네트워크 필터 드라이버(404)일 수 있으며, 상기 제어 수단은 사용자가 콘텐트를 선택하면 자동으로 활성화되어 응용프로그램(144)을 기동시키고, DRM 서버(130)에 접속하여 콘텐트 및 사용자 인증을 수행한 후 복호화키를 포함한 라이센스 패키지(143)를 수신하며, 응용프로그램(144)의 종료에 따라 필터링 동작을 종료시키며, 상기 필터링 수단을 제어하는 DRM 제어기(141)일 수 있고, 상기 응용프로그램(144)은 전용 뷰어 프로그램이 아닌 그 콘텐트를 플레이할 수 있는 운영체제에 등록되어 있는 일반 응용프로그램임이 바람직하다.
그리고, 정보제공 시스템의 상기 콘텐트 서버(122)는 실제 스트리밍이 제공되는 스트리밍 서버(122a)와, 암호화된 콘텐트를 선택할 수 있는 웹 서버(122b) 또는 FTP 서버로 구성함이 바람직하다.
또한, 클라이언트 시스템의 상기 네트워크 필터 드라이버(404)는 응용프로그램(144) 방향으로 네트워크 드라이버의 상단에 위치할 수 있으며, TCP 프로토콜 또는 부가적으로 수신 데이터의 수정기능을 더욱 구비한 UDP 프로토콜을 사용하도록 구성하는 것이 바람직하다.

한편, VOD 스트리밍의 경우에는 상기 콘텐트는 미리 제작된 원본 콘텐트일 수 있고, 라이브 스트리밍의 경우에는 상기 콘텐트는 미리 제작된 원본 콘텐트가 아니라, 동영상 수신장치와 엔코딩 시스템을 통하여 입력되는 실시간 라이브 콘텐트일 수 있으며, 상기 실시간 라이브 콘텐트를 외부 스트리밍 서버로 전송하기 이전에 엔코딩 시스템의 네트워크 드라이버 상단에 설치되는 실시간 후킹과 암호화를 위한 네트워크 필터 드라이버를 더욱 구비하도록 구성함이 바람직하다.
한편, 스트리밍에 의하여 전송되는 암호화된 콘텐트 패키지(142)는 적어도 암호화된 콘텐트(142a)인 데이터 오브젝트 부분과, 암호화되지 않은 메타 데이터(142b)인 헤더 오브젝트 부분으로 구성된다.
여기서, 일 실시예에 의하면, 상기 암호화된 콘텐트 패키지(142)의 DRM 패키지 헤더는 멀티미디어 콘텐트 파일포맷의 헤더 오브젝트에 기록될 수 있고, 상기 DRM 패키지 헤더에는 버전 번호, 콘텐트 URI 길이, 콘텐트 타입 길이, 콘텐트 URI, 콘텐트 타입, 헤더 길이, 데이터 길이, 암호화 방법, 권리 발행자 URL, 콘텐트 이름, 콘텐트 설명, 콘텐트 벤더, 아이콘 URI, 디지털 서명, 콘텐트 서버 URL의 정보가 기록될 수 있도록 구성함이 바람직하다.
또한, 상기 암호화된 콘텐트 패키지(142) 중에서 상기 암호화된 콘텐트(142a) 부분인 데이터 오브젝트는 암호화되고, 응용 프로그램(144)과 콘텐트 서버(122)가 통신하는데 필요한 제어정보이며 헤더인 메타 데이터(142b) 부분은 암호화되지 않도록 처리될 수 있고, 상기 암호화된 콘텐트(142a) 부분인 데이터 오브젝트는 그 내용의 전부가 암호화되거나 또는 미리 정해진 프레임 단위로 일부만 암호화될 수 있으며, 상기 클라이언트 시스템에는 암호화된 콘텐트 패키지(142)를 하드디스크에 저장하는 수단을 더 포함할 수 있도록 구성함이 바람직하다.
또한, 사용자의 인증요청에 따라 클라이언트 시스템으로 전송되는 암호화된 라이센스 패키지(143)는 적어도 암호를 풀기 위한 복호화키(143a) 부분과, 콘텐트의 사 용횟수와 사용기간, 단말기 제한 정보를 포함하는 사용권한에 관한 정보(143b) 부분으로 구성된다.
한편, 본 발명에 의한 스트리밍 콘텐트의 정보보호 방법은
각각 CPU, 휘발성 저장장치(메모리), 비휘발성 저장장치(하드디스크), 입출력장치(키보드, 모니터 등)를 가지며, 유무선 내부 통신수단이나 외부 네트워크와의 통신수단에 의하여 연결되어 있는 정보제공 시스템과 클라이언트 시스템을 이용하여 스트리밍되는 콘텐트의 정보를 보호하는 방법에 있어서,
콘텐트 소스(111)를 암호화하여 암호화된 콘텐트 패키지(121)로 만들어 콘텐트 서버(122)에 업로드하는 암호화 및 업로드 단계와;
사용자가 웹 서버(122b) 또는 FTP 서버에서 선택함에 의하여 스트리밍 서버(122a)에 클라이언트 시스템을 연결하는 시작 및 연결 단계;
스트리밍되는 콘텐트 데이터를 복호화하면서 응용프로그램(144)을 통하여 플레이하는 복호화 및 플레이 단계;
DRM 제어기(141)가 응용프로그램(144)의 종료 메시지를 감지하여 종료하면서 스트리밍 서버(122a)와의 연결을 해제하는 종료 및 연결해제 단계;
로 구성됨을 특징으로 한다.
여기서, 일 실시예에 의하면, 상기 암호화 및 업로드 단계는
콘텐트 패키저(112)가 DRM 서버(130)에 인증 요청을 하는 단계(S201)와;
이에 대하여 DRM 서버(130)가 콘텐트 패키저(112)에 인증 결과를 보내는 단계(S202)와;
콘텐트 패키저(112)가 DRM 서버(130)에 암호화키 요청을 하는 단계(S203)와;
이에 대하여 DRM 서버(130)가 콘텐트 패키저(112)에 암호화키를 보내는 단계(S204)와;
상기 암호화키를 이용하여 콘텐트 패키저(112)가 콘텐트를 블록 암호화 알고리즘을 사용하여 암호화하는 단계와;
콘텐트 패키저(112)가 스트리밍 서버(122a)에 인증 요청을 하는 단계(S205)와;
이에 대하여 스트리밍 서버(122a)가 콘텐트 패키저(112)에 인증 결과를 보내는 단계(S206)와;
콘텐트 패키저(112)가 스트리밍 서버(122a)에 암호화된 콘텐트 패키지(121)를 보내는 단계(S207);
로 구성됨이 바람직하다.
또한, 일 실시예에 의하면, 시작 및 연결 단계, 복호화 및 플레이 단계, 종료 및 연결해제 단계는 순차적으로
사용자의 콘텐트 선택에 의하여 웹 서버(122b) 또는 FTP 서버가 DRM 제어기(141)에 콘텐트 식별정보와 사용자 식별정보를 보내는 단계(S301)와;
DRM 제어기(141)가 DRM 서버(130)에 콘텐트 및 사용자의 인증을 요청하는 단계(S302)와;
DRM 서버(130)가 DRM 제어기(141)에 복호화키 및 사용권한 정보 등 라이센스 인증 내용을 보내는 단계(S303)와;
DRM 제어기(141)가 응용프로그램(144)을 기동시키고, 스트리밍 서버(122a)의 URL 을 전달하는 단계(S304)와;
응용프로그램(144)이 스트리밍 서버(122a)에 콘텐트 데이터를 요청하는 단계(S305)와;
DRM 제어기(141)가 응용프로그램(144)의 종료 명령을 검출(S307)할 때까지 스트리밍 서버(122a)가 응용프로그램(144)에 제어정보와 데이터 패킷을 주기적으로 전송하고, 이 데이터 패킷이 네트워크 필터 드라이버(404)에 의하여 복호화되어 플레이되는 단계(S306)와;
DRM 제어기(141)가 응용프로그램(144)의 종료 명령을 검출하면, 응용프로그램(144)을 종료시키고, 스트리밍 서버(122a)와의 연결을 해제시키는 단계;
로 구성됨이 바람직하다.
여기서, 일 실시예에 의하면 상기 시작 및 연결 단계는
사용자의 콘텐트 선택에 의하여 응용프로그램(144)의 기동과 핸들러의 검사, 프로세스의 등록을 행하는 연결준비 단계와;
이 후의 프로세스의 등록, 리모트 포트의 확인 및 저장을 행하는 연결 단계로 구성됨이 바람직하다.
이때, 일 실시예에 의하면 연결준비 단계는

사용자가 콘텐트를 선택함(701)에 의하여 DRM 제어기(141)가 응용프로그램(144)을 기동시킨 후 일시 정지시키는 단계와;
DRM 제어기(141)가 네트워크 필터 드라이버(404)를 이용하여 응용프로그램(144)과 네트워크 드라이버 사이의 메시지를 후킹하여 핸들러가 0(제로)인지를 판단하는 단계와;
핸들러가 0이면 연결을 단절하기 위하여 어드레스 핸들을 삭제한 후 네트워크 드라이버에 메시지를 전달하고, 핸들러가 0이 아니면 진행하여 다시 네트워크 필터 드라이버(404)에 프로세스가 등록되어 있는지를 판단하는 단계와;
프로세스가 등록되어 있지 않으면 네트워크 드라이버에 그대로 메시지를 전달하고, 프로세스가 등록되어 있으면 어드레스 핸들을 등록하고, 마이이벤트 핸들러를 설정하며, 로컬 포트를 저장한 후에 네트워크 드라이버에 변경된 메시지를 전달하는 단계와;
메시지의 전달에 의하여 응용프로그램(144)이 네트워크 드라이버로부터 준비완료 메시지를 전달받는 단계;
로 구성됨이 바람직하다.
그리고, 일 실시예에 의하면 연결 단계는
네트워크 필터 드라이버(404)가 응용프로그램(144)과 네트워크 드라이버 사이의 메시지를 후킹하여 네트워크 필터 드라이버(404)에 프로세스가 등록되어 있는지를 판단하는 단계(801)와;
프로세스가 등록되어 있지 않으면 네트워크 드라이버에 그대로 메시지를 전달하고, 프로세스가 등록되어 있으면 다시 리모트 포트가 미리 정해져 있는 번호인지를 판단하는 단계와;
리모트 포트의 번호가 미리 정해져 있는 번호가 아니면 네트워크 드라이버에 그대 로 메시지를 전달하고, 리모트 포트의 번호가 미리 정해져 있는 번호이면 그 리모트 포트에 연결된 로컬 포트를 가진 어드레스 핸들 구조체에 리모트 포트 번호를 저장한 후 네트워크 드라이버에 그대로 메시지를 전달하는 단계;
로 구성됨이 바람직하다.
한편, 일 실시예에 의하면 복호화 및 플레이 단계는
네트워크 드라이버가 네트워크를 통하여 스트리밍 방식으로 데이터를 수신하는 단계(901)와;
마이이벤트 핸들러가 활성화되어 리모트 포트가 미리 정해져 있는 번호인지를 판단하는 단계와;
리모트 포트가 미리 정해져 있는 번호가 아니면 응용프로그램(144)에 데이터를 그대로 전송하고, 리모트 포트가 미리 정해져 있는 번호이면 응용프로그램(144)에 데이터를 복호화(905)한 후에 전송하는 단계;
로 구성됨이 바람직하다.
여기서, 일 실시예에 의하면, 상기 복호화(905)를 하기 전에 하드디스크에 저장할 것인지의 여부를 판단하는 단계와;
하드디스크에 저장할 것이라고 선택되지 않은 경우에는 그대로 복호화(905)하고, 하드디스크에 저장할 것이라고 선택된 경우에는 하드디스크에 암호화된 콘텐트를 저장한 후에 복호화(905)를 행하도록 하는 단계;
를 더욱 구비하여 구성될 수 있다.
한편, 일 실시예에 의하면 종료 및 연결해제 단계는
콘텐트 데이터를 복호화하고 플레이하는 매 주기마다 DRM 제어기(141)가 응용프로그램(144)의 종료 메시지를 검출하는 단계와;
종료 메시지가 검출되지 않으면 다시 복호화 및 플레이 단계로 진행하고, 종료 메시지가 검출되면 응용프로그램(144)을 종료시키고, 어드레스 핸들을 삭제함으로써 스트리밍 서버(122a)와의 연결을 해제시키는 단계;
로 구성됨이 바람직하다.
그리고, 본 발명에 의한 방법이 기록된 기록매체는
각각 CPU, 휘발성 저장장치(메모리), 비휘발성 저장장치(하드디스크), 입출력장치(키보드, 모니터 등)를 가지며, 유무선 내부 통신수단이나 외부 네트워크와의 통신수단에 의하여 연결되어 있는 정보제공 시스템과 클라이언트 시스템을 이용하여 스트리밍되는 콘텐트의 정보를 보호하는 방법이 저장된 컴퓨터로 실행할 수 있는 기록매체에 있어서,
콘텐트 소스(111)를 암호화하여 암호화된 콘텐트 패키지(121)로 만들어 콘텐트 서버(122)에 업로드하는 암호화 및 업로드 단계와;
사용자가 웹 서버(122b) 또는 FTP 서버에서 선택함에 의하여 스트리밍 서버(122a)에 클라이언트 시스템을 연결하는 시작 및 연결 단계;
스트리밍되는 콘텐트 데이터를 복호화하면서 응용프로그램(144)을 통하여 플레이하는 복호화 및 플레이 단계;
응용프로그램(144)의 종료 메시지를 감지하여 종료하면서 스트리밍 서버(122a)와의 연결을 해제하는 종료 및 연결해제 단계;
로 구성됨을 특징으로 하는 스트리밍 콘텐트의 정보보호 방법이 저장되어 있는 컴퓨터로 실행할 수 있는 기록매체이다.
이하, 상기와 같은 구성을 가지는 본 발명의 내용을 첨부된 도면을 참조하여 보다 상세히 설명한다.
상술한 본 발명의 목적, 특징 및 장점들은 하기의 첨부된 도면과 상세한 설명을 통해서 본 발명의 바람직한 일 실시예인 마이크로소프트의 윈도우 운영체제(Operating System, OS)에 대해서 구체화될 것이다.
그러나 본 발명에서 구체적으로 제시된 기술적 사상을 이용하면 마이크로소프트의 윈도우 운영체제이외의 매킨토시, 리눅스, 유닉스와 같은 다른 운영체제를 사용하는 정보제공 시스템과 클라이언트 시스템에도 쉽게 적용할 수 있다는 것은 당업자라면 쉽게 알 수 있을 것이다. 또한 본 발명에서의 클라이언트 시스템이란 유무선 인터넷으로 연결되어 스트리밍 방식으로 제공되는 멀티미디어 콘텐트를 사용할 수 있는 PC이외의 노트북, PDA, 휴대폰, 셋톱박스, 디지털 TV, 텔레메틱스 단말기를 포함하는 개념인 것을 미리 밝혀두는 바이다.
도 1은 본 발명의 디지털 저작권 관리(DRM) 시스템의 전체 모식도이다.

먼저 스트리밍 서비스가 가능한 동영상이나 영화, 음악, 온라인교육과 같은 멀티미디어 콘텐트 소스(111)를 암호화 수단(110)인 콘텐트 패키저(Content Packager, 112)가 DRM 서버(130)로부터 발급받은 암호화키를 이용하여 암호화된 콘텐트 패키지(121)로 생성하여 공급 수단(120)인 콘텐트 서버(122)에 올리게 된다. 콘텐트 서버(122)는 웹(122b) 또는 FTP, 스트리밍 서버(122a) 등으로 구성할 수 있으며, DRM 클라이언트 시스템(140)의 사용자(401)가 콘텐트 서버(122), 예컨대 웹 서버(122b)와 접속하여 관심있는 콘텐트 이름을 선택하면 DRM 제어기(141)가 가동하여 콘텐트 서버, 예컨대 스트리밍 서버(122a)로부터 암호화된 콘텐트 패키지(142)를 수신하게 된다. 여기서 콘텐트 패키지(121)와 암호화된 콘텐트 패키지(142)는 모두 암호화된 상태의 콘텐트 패키지이지만 일반적으로 같지 않게 된다. 즉 콘텐트 서버의 콘텐트 패키지(121)는 스트리밍 서버가 인터넷의 전송율에 따라 각각 다른 전송율을 선택하여 콘텐트 데이터를 클라이언트 시스템에 송신하게 되므로 각 전송율에 따른 데이터와 정보를 모두 가지고 있지만, 실제 클라이언트 시스템에서 수신받은 암호화된 콘텐트 패키지(142)는 변화되는 전송율에 따라 수신받은 해당 데이터만을 가지고 있기 때문이다.

클라이언트 시스템에서 수신받은 암호화된 콘텐트 패키지(142)는 원본 멀티미디어 콘텐트(111)를 암호화시킨 콘텐트(142a)와 암호화된 콘텐트 패키지(142)에 대한 각종 정보를 가지고 있는 헤더인 메타데이터(142b)로 구성된다.

또한, 클라이언트 시스템(140)의 사용자(401)가 암호화된 콘텐트 패키지(142)를 사용하기 위해서는 DRM 서버(130)의 DRM 라이센스 발급기(DRM License Issuer, 133)로부터 복호화키(143a)와 사용횟수, 사용기간, 단말기 제한 등의 사용권한(143b)에 대한 정보로 구성된 암호화된 라이센스 패키지(143)를 제공받아야 한다.

그 후, 클라이언트 시스템(140)의 인증기(145)가 라이센스 패키지(143)의 사용권한 분석을 수행하며, 정당한 사용권한이 있는 사용자(401)라고 인정되면 DRM 제어 기(141)가 직간접으로 복호화키(143a)를 이용하여 암호화된 콘텐트 패키지(142)를 복호화한 후, 콘텐트를 볼 수 있는 기존의 응용프로그램(144)으로 전달하게 된다. 이러한 DRM 시스템에서의 DRM 서버(130)는 암호화된 콘텐트 패키지(142)를 생성하기 위한 암호화키의 생성 및 발급, 관리, 라이센스 관리, 사용자 인증, 사용자 컴퓨터의 하드웨어 인증, 응용프로그램 인증 등의 역할을 수행하게 된다.

상기 DRM 서버(130)는 각종 데이터 정보를 보관하는 DRM 서버 DB(131)와; 콘텐트 패키저(112)와 콘텐트 서버(122), 클라이언트 시스템(140), 빌링 서버(150) 등과 네트워크를 통한 각종 정보교환을 위한 DRM 서버 콤포넌트(132)와; 라이센스 발급을 담당하는 DRM 라이센스 발급기(133)와; DRM 서버(130)의 각종 설정 관리와 회원관리, 콘텐트 관리, 로그 분석 등을 해 줄 수 있는 관리자 프로그램(administrator program)인 DRM 관리기(134)로 구성된다. 만약 콘텐트 제공 서비스가 유료화된 것이라면 후불제 방식의 빌링 서버(150) 또는 선불제 방식의 페이먼트 게이트웨이 서버(160)를 통해 과금이 이루어지게 된다.

도 1의 전체 DRM 시스템은 상당히 복잡하지만 크게 분류해 보면 콘텐트 제공 시스템(110, 120, 130)과 클라이언트 시스템(140)의 2가지로 나눌 수 있다. 암호화된 콘텐트 패키지(121)를 생성하고 고객, 즉 콘텐트 사용자(401)들에게 서비스할 수 있도록 준비하는 콘텐트 제공 시스템은 암호화 수단(110)인 콘텐트 패키저(112)와 공급 수단(120)인 콘텐트 서버(122), 그리고 DRM 서버(130)로 구성된다. 여기서 콘텐트 패키저와 콘텐트 서버(웹, 스트리밍, FTP서버), DRM 서버는 각각 소프트웨어로 구성되어 있으며, 하나의 컴퓨터에 일체화되어 설치될 수도 있으며 효율성을 높 이기 위해 각각 다른 컴퓨터를 사용할 수도 있다. 한편, 클라이언트 시스템(140)은 암호화된 콘텐트 패키지(142)를 유무선 인터넷 또는 네트워크망을 통해 제공받아 복호화하여 사용할 수 있도록 기능을 제공하는 DRM 제어기(141)가 핵심적인 역할을 담당하게 된다.

도 2는 콘텐트 제공 시스템에서의 암호화된 콘텐트 패키지(121)의 생성과정, 즉 암호화 및 업로드 단계의 과정을 보여주는 모식도이다.

본 도면에서는 표시되지 않았지만, 먼저 콘텐트 제공 시스템의 구성요소가 되는 콘텐트 패키저(112), DRM 서버(130), 콘텐트 서버(122) 프로그램을 각각 설치하고, 기본적인 시스템 설정작업을 수행해 놓는다. 그 후 콘텐트 패키저(112) 프로그램을 실행하면, DRM 서버(130)와 접속하기 위한 사용자(401)의 아이디와 비밀번호를 통한 인증과정(S201)을 거친다.

그 후, DRM 서버(130)가 콘텐트 패키저(112)의 사용자 인증을 수행한 후 인증결과(S202)를 전달하면, 콘텐트 패키저(112)의 사용자(401)는 암호화할 원본 콘텐트(111)를 선정하여 DRM 서버(130)에 암호화키를 요청(S203)한다. DRM 서버(130)는 예컨대 의사랜덤숫자(Pseudorandom Number) 발생 알고리즘을 이용하여 랜덤한 암호화키를 생성시키고, 이 암호화키를 콘텐트 패키저(112)에게 전달(S204)한다. 그러면 콘텐트 패키저(112)는 전달받은 암호화키를 이용하여 원본 콘텐트(111)를 암호화하여 암호화된 콘텐트 패키지(121)를 생성시킨다. 이때 암호화 패키저는 파일 단위 또는 여러개의 파일이 동시에 포함되어 있는 디렉토리를 통째로 암호화를 진행시킬 수 있다.

이때 암호화를 위해서는 보안성과 효율성이 우수한 블록암호화(Block Cipher) 알고리즘을 사용하여 멀티미디어 콘텐트를 블록단위로 암호화하는 것이 바람직하다. 또한 암호화키 및 복호화키의 교환방식은 비밀키(Private Key)나 공개키(Public Key) 전송방식 어느 쪽을 사용하더라도 무방하게 구현할 수 있다. 그리고 스트리밍 방식으로 멀티미디어 콘텐트를 서비스하기 위한 원본 콘텐트(111)의 헤더 정보는 그대로 놓아두고, 데이터 부분을 찾아서 전부 또는 일부분 암호화를 수행하는 것이 바람직하며, 이에 대한 자세한 설명은 추후에 될 것이다. 또한 암호화된 콘텐트 패키지에 관련한 각종 메타데이터는 별도의 DRM 패키지 헤더로 만들어 삽입하게 된다.

그 후, 암호화된 콘텐트 패키지(121) 파일을 스트리밍 서버(122a)에 올려놓기 위하여 콘텐트 패키저(112)의 사용자는 스트리밍 서버(122a)에 접속하여 FTP(File Transfer Protocol)를 이용하기 위한 사용자 인증(S205)을 수행하고, 인증결과를 수신(S206)한 후, 암호화된 콘텐트 패키지(121) 파일을 스트리밍 서버(122a)에 업로드(S207)하게 된다. 여기서는 일 실시예로서 FTP 방식으로 콘텐트를 업로드하는 것에 대해 설명했지만, 내외부 네트워크로 연결하여 쉽게 파일복사 방식으로도 업로드할 수 있다. 이로써 암호화 및 업로드 단계가 종료된다.

여기서 스트리밍의 과정을 잠시 고찰한다. 일반적으로 인터넷을 통한 스트리밍 방식의 콘텐트 서비스는 다음과 같은 과정을 통해 이루어진다.
먼저 콘텐트 제공자는 동영상, 영화, 음악과 같은 스트리밍 서비스를 할 수 있는 멀티미디어 콘텐트를 스트리밍 서버(122a)에 올려놓고, 이 스트리밍 서버(122a)의 URL 등의 정보를 링크해 놓은 웹 서버(122b)에 콘텐트를 게시하게 된다. 그러면 클라이언트 시스템(140)의 사용자(401)는 콘텐트 제공자의 웹 서버(122b)에 접속하여 회원가입을 하고, 이때 부여받은 아이디와 비밀번호를 이용해서 인증과정을 거친다.
이렇게 사용자가 인증과정을 거친 후에 웹 서버(122b)의 웹페이지 상의 원하는 멀티미디어 콘텐트를 선택하면, 콘텐트 포맷의 확장자에 따른 클라이언트 시스템(140)의 해당 콘텐트를 플레이할 수 있는 응용 프로그램(144)이 활성화되고, 상기 응용 프로그램(144)에 스트리밍 서버(122a)의 URL 정보가 전달되게 된다. 그 후 해당 응용 프로그램(144)은 스트리밍 서버(122a)와 서로 통신하면서 콘텐트를 최적의 상태로 볼 수 있도록 지원하는 제어 정보와 실제의 콘텐트 데이터를 전달받게 되는 것이다.
도 3은 사용자가 스트리밍 방식으로 암호화된 멀티미디어 콘텐트를 플레이하는 과정을 보여주는 모식도이다.
참고적으로, 클라이언트 시스템(140)에 DRM 제어기(141)가 미리 설치되어 있지 않은 경우에는 사용자(401)가 콘텐트 제공자의 웹페이지에 처음 접속하여 회원가입하거나, 또는 DRM이 적용된 콘텐트를 선택하여 사용하고자 할 때 ActiveX 콘트롤 방식으로 단 한번만 설치해 주게 된다. 또한 추후 DRM 제어기(141)의 버전이 업그레이드되었을 때에는 버전을 비교하여 자동으로 업그레이드될 수 있도록 구현할 수도 있다.
먼저, 도면에서는 표시하지 않았지만, 클라이언트 시스템(140)의 사용자(401)가 웹 페이지에 접속하여 사용자 인증과정을 거친 후, 웹페이지의 콘텐트를 선택하게 된다. 그 후 웹 서버(122b)는 해당 콘텐트에 대한 식별정보와 웹페이지에서의 인증과정을 통해 확보한 아이디 및 비밀번호를 클라이언트 시스템(140)의 DRM 제어기(141)에 전송(S301)한다.
상기 DRM 제어기(141)는 웹 서버(122b)로부터 전송받은 상기 정보를 DRM 서버(130)로 전송(302)하여 사용자 인증 및 콘텐트의 식별정보를 확인하고 난 후, 정당한 사용권한이 있는 사용자(401)라면 복호화키(143a)와 사용권한(143b)에 대한 라이센스 인증결과를 암호화된 라이센스 패키지(143) 형태로 다시 DRM 제어기(141)로 전송(S303)한다. 그러면 상기 DRM 제어기(141)는 전송받은 라이센스 인증결과를 바탕으로 해당 콘텐트 파일 포맷을 지원하는 기존의 응용프로그램(144)을 가동시키고, 스트리밍 서버(122a)의 URL 정보를 해당 응용프로그램(144)에 전달(S304)한다.
그 후 상기 응용프로그램(144)은 클라이언트 시스템(140)의 외부 네트워크망과 통신할 수 있는 장치를 이용하여, 스트리밍 서버(122a)에 해당 콘텐트 데이터를 송신해 달라고 요청(S305)하며, 이에 의하여 상기 스트리밍 서버(122a)는 주기적으로 응용프로그램(144)과 통신하면서 해당 콘텐트 데이터를 전송(S306)하게 되고, 이렇게 전송된 암호화된 데이터(142)는 복호화되어 응용프로그램(144)에 의하여 플레이될 수 있게 된다.
이렇게 스트리밍 방식으로 데이터가 전송되는 동안 DRM 제어기(141)는 사용자(401)가 응용 프로그램(144)을 종료한다는 메시지를 발생시키는지 여부를 감시하고 있다가, 종료 메시지를 감지하게 되면 그 응용 프로그램(144)을 종료(S307)하게 되는 것이다.
여기서 주의할 것은, 본 발명의 기술 내용에서의 응용 프로그램(144)은 기존의 DRM 시스템에서처럼 복호화 알고리즘을 포함하고 있는 "전용 뷰어 프로그램"이 아니라, 암호화되기 이전의 원본 멀티미디어 콘텐트(111)를 플레이하기 위한 기존의 일반적인 뷰어 또는 플레이어 프로그램을 의미한다. 즉 본 발명의 클라이언트 시스템(140)의 DRM 제어기(141)와 이에 의하여 제어되는 네트워크 필터 드라이버(404)가 기존의 응용프로그램(144)을 제어하면서 스트리밍 방식으로 전달되는 암호화된 콘텐트 패키지(142)의 데이터를 복호화하여 응용프로그램(144)에 전달해 주기 때문에, 응용프로그램(144)의 입장에서는 네트워크 필터 드라이버(404)를 통해 전달받는 복호화된 데이터가 원래 암호화되었던 것인지 아닌지를 전혀 판별하지 못하게 된다.
그리고, 본 발명에서는 DRM 제어기(141)가 스트리밍 방식의 멀티미디어 콘텐트를 볼 수 있는 응용프로그램(144), 즉 미디어 플레이어인 윈도미디어플레이어 또는 리얼플레이어, 퀵타임플레이어 등을 직접 제어할 수도 있으며, 또 다른 방법으로는 최근에 많이 사용하고 있는 OCX(OLE Custom Control)를 사용하여 웹브라우저 내에 상기 응용프로그램(144)의 콤포넌트를 삽입하여 제작한 뷰어로 구현할 수도 있다.
한편, 응용프로그램(144)과 외부의 스트리밍 서버(122a)가 통신을 하기 위해서는 클라이언트 시스템(140)의 네트워크 장치를 필수적으로 사용하게 되기 때문에, 본 발명에서는 DRM 제어기(141)와 연동되어 작동하는 네트워크 필터 드라이버(404)가 응용프로그램(144)과 네트워크 드라이버 사이의 메시지와 패킷의 후킹 및 변경, 복호화, 전달하는 필터링을 수행하도록 구성함이 바람직하다. 본 도면에 표시되지 않 은 상기 네트워크 필터 드라이버(404)는 별도로 제작하여 삽입하게 되며, 나중에 자세히 설명될 것이다.
도 4는 클라이언트 시스템(140)에서의 스트리밍 콘텐트를 플레이하는 과정의 모식도이다.
여기서는 상술한 바와 같이 클라이언트 시스템(140)의 사용자(401)가 스트리밍 서버(122a)와 연동되어 있는 웹페이지 상의 암호화된 콘텐트(121)를 선택하면, 자동으로 DRM 제어기(141)가 가동되면서 해당 원본 콘텐트를 볼 수 있는 응용프로그램(144)을 활성화시키고, 네트워크 장치를 통해 해당 콘텐트의 데이터를 스트리밍 방식으로 수신하게 되는 것을 보여준다. 상기 클라이언트 시스템(140)은 NIC(Network Interface Card, 402)를 통해 외부 네트워크와 연결되어 있고, NIC(402)를 통해 수신된 데이터는 네트워크 드라이버(403)인 예컨대 TDI (Transport Device Interface) 드라이버(506)로 전달되며, 상기 네트워크 드라이버(403) 상단에 본 발명에서의 네트워크 필터 드라이버(404)를 삽입되고, 이 네트워크 필터 드라이버(404)가 DRM 제어기(141)와 연동되어 메시지와 패킷의 후킹 및 변경, 복호화 작업을 수행한 후에 데이터가 응용 프로그램(144)으로 전달되는 필터링 작업이 수행한다. 여기서 TDI 드라이버의 역할은 네트워크 프로그램의 수행 속도를 향상시키기 위해 커널 모드에서 프로토콜 스택과 통신하는 드라이버를 말

한다.
일반적으로 클라이언트 시스템(140)은 크게 사용자 모드와 커널 모드로 나눌 수 있는데, 사용자 모드에서 작동하는 프로그램은 응용프로그램(144)과 DRM 제어기(141)가 되며, 실제 하드웨어 장치와 밀접한 관련이 있는 하위레벨의 커널 모드에 해당하는 것은 NIC(402), 네트워크 드라이버(403) 및 네트워크 필터 드라이버(404)가 해당된다. 따라서 본 발명에서 클라이언트 시스템(140)에 설치되는 프로그램은 사용자 모드에서 작동하는 DRM 제어기(141)와 커널모드에서 작동하는 네트워크 필터 드라이버(404)로 구성된다.
여기서 잠시 레이어와 네트워크 프로토콜에 대하여 고찰한다.
최근의 멀티미디어를 플레이 할 수 있는 응용 프로그램(144)과 스트리밍 서버(122a)는 인터넷 트래픽 환경을 고려하여 지능적으로 최적의 통신포트를 찾거나 실시간으로 송수신할 콘텐트 데이터의 전송속도와 양을 가변함으로써 최상의 스트리밍 서비스를 할 수 있게끔 지원하고 있다. 이러한 스트리밍을 지원하는 네트워크 전송 프로토콜은 데이터의 전달사항을 감시하며, 여러 가지 제어기능과 매체식별기능을 제공한다. 일반적으로 전송 컴퓨터는 송신할 콘텐트를 패킷(packet)이라는 작은 섹션으로 데이터를 분할하고, 목적지의 컴퓨터가 인식하도록 패킷에 주소정보를 추가하고 네트워크를 통해 전송용 네트워크 카드에 데이터를 전달하는 동작을 한다. 또한 수신 컴퓨터는 NIC로부터 데이터를 전달받고, 송신 컴퓨터에 의해 추가된 정보를 제거하고, 데이터 패킷을 본래의 메시지로 다시 조합하는 동작을 한다. 패킷은 일반적으로 원본 콘텐트의 소스와 어드레스, 전송을 동기화하는 시간정보 등을 포함한 헤더(header), 실제 네트워크에 따라 가변되어 전달되는 실제 전송되는 데이터(data), 통신을 통해 전달된 데이터의 에러정보가 기록된 테일러(tailer)로 구성되어 있다. 이러한 전송 컴퓨터와 수신 컴퓨터의 동작, 패킷 의 구조와 구성정보 등을 규정하는 것이 네트워크 프로토콜이다.
이러한 스트리밍에 관련된 네트워크 기술과 프로토콜은 대부분 인터넷에 관한 국제적 표준화 추진기구인 IETF(Internet Engineering Task Force)에서 표준화된다. IETF에서는 스트리밍 전송을 위한 RTP/RTCP(Realtime Transport Protocol / Realtime Transport Control Protocol)와 스트리밍 제어를 위한 RTSP(Realtime Streaming Protocol) 등을 제정하여 전세계적으로 표준으로 사용하고 있으며, 이러한 네트워크 프로토콜은 하위 전송 프로토콜에 독립적이므로 TCP와 UDP 모두에서 사용될 수 있다.
클라이언트 시스템(140)에서 외부의 전송 컴퓨터로 부터 유무선 인터넷으로 콘텐트의 데이터를 수신받는 것은 네트워크 장치가 담당하며, 이를 구동할 수 있는 각종 네트워크 드라이버들이 커널 모드에서 작동하고 있다.
이러한 커널 모드의 네트워크를 통한 통신은 매우 복잡하기 때문에 국제적으로 특정 정보처리 기기, 하드웨어 또는 소프트웨어의 실제 구조에 의존하지 않는 논리적이고 보편적인 망 모델을 규정하기 위해 ISO 표준인 OSI (Open System Interconnection)의 7층의 계층화된 참조모델(reference model)을 규정하고 있다. 이에 의하면 이 7계층을 하위 4층인 주로 전송처리 규정과 상위 3층인 주로 정보처리 규정으로 나누고, 하위층의 기능을 서브 세트화 함으로써, 전송 형태에 영향받지 않는 전송서비스를 상위층에 제공하는 것이 가능하다. 이러한 OSI의 각 표준규격은 OSI 참조모델에 따라 계층마다 다른 개방형 시스템의 동위 계층과 데이터를 주고받기 위한 프로토콜의 규격과 바로 위의 계층에 제공하는 기능을 규정하고 있 다.
OSI 참조모델의 7 계층을 설명하면, 제1계층인 물리적(physical)층은 물리적인 매체를 통해 비트의 전송 및 수신을 담당하고, 제2계층인 데이터 링크(data link)층은 에러체크 정보를 추가하고 프레임 비트를 구성하며, 제3계층인 네트워크(network)층은 인터네트워크의 시퀀싱, 어드레싱, 라우팅을 담당하고, 제4계층인 전송(transport)층은 인터네트워크의 시퀀싱, 어드레싱, 에러제어 정보를 담당하며, 제5계층인 세션(session)층은 프로세스에 식별자를 추가하고 에러정보를 다루고, 제6계층인 표현(presentation)층은 데이터의 구성을 해석하고 암호화기능을 추가하며, 제7계층인 응용(application)층은 사용자 어플리케이션을 직접 지원하는 서비스를 제공하는 것으로 규정되어 있다. 이 7 계층의 최하위 계층은 하드웨어 연결만을 담당하고, 최상위 계층은 응용 프로그램 레벨의 소프트웨어 상호작용을 담당하게 된다.
물론, 실제 정보처리 기기나 하드웨어, 소프트웨어에서는 실제로 OSI의 7 계층의 참조모델에 따르는 것은 아니지만, 일반화시켜 설명할 때는 상당히 유용한 표준 모델로서의 역할을 담당하고 있다.
상기 OSI(Open System Interconnection) 참조모델의 제3계층에 해당하는 IP(Internet Protocol)는 네트워크 계층에 해당하는 프로토콜이며, IP 주소에 따라 다른 경로제어에 의한 네트워크 간의 패킷 전송을 가능하게 하는 프로토콜이지만, 패킷이 발신된 순서대로 도착하는 것을 보증해 주지는 않는다. 또한 일반적으로 IP는 OSI 기본 참조모델을 기준으로 제4계층인 전송계층에 해당하는 TCP 또는 UDP와 함께 사용하게 된다.
여기서 TCP(Transmission Control Protocol, 전송 제어 프로토콜)는 일반적으로 IP와 함께 TCP/IP를 구성하고 있는 가장 범용적인 전송 제어 프로토콜이며, 패킷의 도착 순서대로 배열이나 오류 수정 등이 행해지므로 TCP보다 상위계층에서 보았을 때는 네트워크로 연결된 2대의 컴퓨터가 신뢰성이 높은 전용선으로 연결된 것과 같은 효과를 보이게 된다. 이와 대비하여 UDP(User Datagram Protocol)는 인터넷의 표준 프로토콜의 집합인 TCP/IP의 기반이 되는 프로토콜의 하나이며, TCP에서는 접속을 설정한 후에 통신을 개시하지만, UDP에서는 세션을 설정하지 않고 데이터를 상대의 주소로 송출한다. 이러한 UDP는 전송데이터의 신뢰성보다는 고속성이 요구되는 멀티캐스팅을 지원하기 위해 많이 사용하는 프로토콜로서, 전송 처리가 고속이라는 장점이 있지만, TCP와 같이 전송데이터의 오류 정정이나 재송신 기능이 없는 것이 단점이다.
도 5는 네트워크의 계층구조에서 네트워크 필터 드라이버(404)의 위치에 관한 모식도이다.
도 5는 본 발명에서의 일 실시예인 윈도 운영체제를 모델로 한 것이며, 여기에서 인터넷과 같은 외부 네트워크 망과 연결되어 수신된 데이터 흐름이 커널 모드에서 NIC(Network Interface Card, 402), NDIS (Network Driver Interface Specification) 프로토콜 드라이버(501), IP(Internet Protocol, 502), TCP(Transmission Control Protocol, 503) 또는 UDP(User Datagram Protocol, 504), TDI 드라이버(506), 네트워크 필터 드라이버(404), I/O Manager(Inp

ut/Output Manager, 505) 순으로 전달되는 것을 간략하게 도시한 것이다.
여기서 NIC(402)는 주로 네트워크와 연결되어 비트를 전송하고 전송받는 네트워크 인터페이스 카드가 되며, NDIS 프로토콜 드라이버(501)는 마이크로소프트의 네트워크 인터페이스 드라이버이다. 그리고 IP(502)는 상술한 바와 같이 상위 층인 TCP(503) 또는 UDP(504)와 함께 네트워크 간의 패킷전송을 담당한다. 또한 TCP와 UDP의 상단에 위치하는 TDI 드라이버(506)는 상위 응용프로그램과 네트워크를 통한 외부 전송 시스템과의 통신을 담당하는 대표적인 네트워크 드라이버(403)이며, 네트워크 필터 드라이버(404)는 응용프로그램(144) 방향으로 TDI 드라이버(506)의 상단에 위치하게 된다. 왜냐하면 TDI 드라이버(506)단에서 TCP와 UDP를 통해 무질서하게 수신된 데이터 패킷을 정리하여 통과시켜 주기 때문에 네트워크 필터 드라이버(403)는 그 위에 위치시키는 것이 바람직하다. 그리고 커널레벨의 가장 상단에 위치하는 I/O Manager(505)는 하위 레벨의 각종 드라이버를 로드하고 관리하는 역할을 담당한다.
이와 같이 본 발명의 핵심 부분인 네트워크 필터 드라이버(404)는 응용프로그램(144)과 TDI 드라이버(506)의 사이에 위치하면서 메시지와 데이터 패킷의 후킹 및 변경, 복호화, 전달하는 필터링 작업을 수행하게 된다.
그런데, 일반적으로 인터넷 방송을 통한 스트리밍 콘텐트의 전송을 위해서는 신뢰성이 보장되는 TCP를 많이 사용하지만, 음악공연 또는 실시간 스포츠 중계를 위해서는 고속전송을 위해서는 UDP를 사용하기도 한다. 따라서 본 발명에서의 스트리밍 데이터의 전송 프로토콜은 각각 TCP를 이용하거나, 또는 UDP를 이용할 수 있게 구현하게 된다.
물론 네트워크 필터 드라이버(404)가 복호화를 수행할 때 TCP로 전송되는 것이라면 이미 TDI 드라이버(506) 상단에서는 패킷의 도착 순서대로 배열이나 오류수정 등이 행해진 상태이므로 암호화된 데이터를 연속적으로 복호화하여 응용프로그램으로 전송하면 된다. 그러나 UDP로 전송되는 경우에는 고속전송에 따른 데이터의 오류 또는 배열을 수정하는 기능을 네트워크 필터 드라이버(404)에 부가적으로 더 구비해야 한다.
도 6은 암호화된 스트리밍 콘텐트 데이터의 이동과정을 보여주는 모식도이다.
일단 클라이언트 시스템(140)으로 네트워크망을 통해 암호화된 콘텐트 패키지(142)의 데이터가 전송되면 각각 NIC(402), 네트워크 드라이버(403), 네트워크 필터 드라이버(404), I/O 매니저(505), OS 또는 플랫폼 API(604) 등의 경로를 거쳐서 응용프로그램(144)으로 전달된다. 그런데 본 발명에서의 클라이언트 시스템(140)의 핵심 요소는 사용자 모드에서 작동하는 DRM 제어기(141)와 커널 모드에서 작동하는 네트워크 필터 드라이버(404)로 구성된다.
좀 더 구체적으로 고찰하면, 사용자 모드에서 작동하는 DRM 제어기(141)는 본 도면에서는 표시되지 않은 DRM 서버(130)와 연결되어 불법복제 프로그램의 접근을 방지하기 위한 접근허용 검사 및 사용자 인증, 클라이언트 단말기의 하드웨어 인증, 라이센스 조회 및 사용권한 조사, 복호화키의 수신, 네트워크 필터 드라이버(404)의 가동 및 제어 등의 역할을 담당하게 된다. 또한 커널모드에서 작동하는 네트워 크 필터 드라이버(404)는 네트워크 드라이버(403)의 상단에 위치하여 응용프로그램(144)과 네트워크 드라이버(403) 사이의 메시지와 패킷의 후킹, 새로운 이벤트의 발생, 네트워크 연결의 변경, 암호화된 데이터의 식별, 암호화된 데이터의 복호화, 복호화된 데이터의 응용 프로그램(144)에게로의 전달 등의 필터링 작업을 수행하게 된다.
만약 네트워크 필터 드라이버(404)의 상단에 새로운 디바이스 드라이버가 로딩되는 것을 허용하면 복호화된 콘텐트를 해킹당할 수 있다는 보안상의 취약점이 발생하므로, 네트워크 필터 드라이버(404)는 다른 디바이스 드라이버의 로딩을 감시하고 있다가 만약 상단에 다른 드라이버가 로딩되는 것을 감지하면 동작을 멈추는 기능도 구비하여야 한다. 또한 클라이언트 시스템(140)의 사용자(401)가 응용프로그램(144)의 종료 메시지를 발생시키는지 여부를 감시하는 기능도 구비하여야 한다.
실제에 있어서는 상술한 DRM 제어기(141)와 네트워크 필터 드라이버(404)의 대부분의 많은 기능들은 사용자 모드와 커널모드 어느 쪽에서 구현되더라도 크게 문제가 되지는 않는다.
그리고 상술한 바와 같이 스트리밍 방식으로 콘텐트 데이터가 클라이언트 시스템(140)으로 원활하게 수신되기 위해서는 응용프로그램(144)과 외부의 스트리밍 서버(122a)가 지능적으로 통신 및 데이터의 수신을 수행하게 된다. 이러한 외부 스트리밍 서버(122a)와의 각종 통신 환경의 설정을 지원해 주는 역할은 네트워크 드라이버(403)가 담당하고 있다. 따라서 응용 프로그램(144)과 네트워크 드라이버(403)사이에 본 발명의 네트워크 필터 드라이버(404)가 위치하게 되는 것이 바람직하며, 응용프로그램(144)과 네트워크 드라이버(403)가 주고 받는 메시지와 패킷을 후킹 및 변경, 복호화, 전달하는 필터링 작업을 수행하게 된다.
그런데, 응용 프로그램(144)이 외부 스트리밍 서버(122a)로부터 수신받는 데이터(142)는 크게 실제 동영상 등에 해당하는 콘텐트 데이터(142a, 601)와, 이 콘텐트의 원활한 서비스를 제어하기 위한 제어 정보(142b, 602)로 나뉠 수 있다. 본 발명에서의 중대한 특징 중의 하나는 이 중의 콘텐트 데이터만 암호화하고, 제어 정보는 암호화하지 않은 상태로 스트리밍 서버(122a)에서 클라이언트 시스템(140)의 응용 프로그램(144)으로 전송하도록 함으로써, 기존의 스트리밍 서비스를 위하여 설치되어 있는 서버나 네트워크에 과부하를 발생하지 않고도 암호화된 콘텐트를 서비스할 수 있도록 지원한다는 점이다.
도면에서 암호화된 콘텐트 데이터(601)는 네트워크 필터 드라이버(404)에서 복호화 작업이 수행되고, 이 복호화된 콘텐트 데이터(603)가 응용 프로그램(144)에까지 전달되는 것을 도시하고 있다. 반면에 원활한 스트리밍을 지원하기 위한 제어정보(602)는 암호화되지 않은 상태로 응용 프로그램(144)에게로 전달되게 된다.
이제 네트워크 필터 드라이버의 동작에 대하여 고찰한다.
일반적으로 웹페이지의 스트리밍 콘텐트를 클라이언트 시스템(140)의 사용자(401)가 클릭을 하면, 그 콘텐트의 파일 포맷을 지원하는 응용프로그램(144)이 활성화되고, 해당 응용 프로그램(144)이 네트워크 드라이버(403)에 스트리밍 서버(122a)와 연결할 수 있는 준비를 하며, 이렇게 연결이 확인되고 나면 스트리밍 방식으로 데이터를 수신하게 된다.

그러나 파일 필터 드라이버가 응용 프로그램과 파일시스템 사이의 일대일 대응관계를 가지는 동기화된 메시지와 데이터를 후킹하고 필터링하는 것과는 다르게, 네트워크 필터 드라이버(404)는 응용 프로그램(144)과 외부의 스트리밍

서버(122a)를 제어하는 네트워크 드라이버(403) 사이에서 발생하는 일대다 형태의 대응관계를 가지는 비동기화된 메시지 및 데이터 패킷의 후킹과 변경, 복호화, 전달하는 필터링을 수행해 주어야 하는 복잡성이 있다. 왜냐하면 최근의 컴퓨터들은 기본적으로 멀티태스킹을 지원하기 때문에 네트워크를 통해 다양한 데이터의 송수신이 이루어지고 있으며, 또한 스트리밍 기술의 급속한 발전에 의해 인터넷 트래픽 환경에 따라 지능적으로 전송속도를 가변하여 하나 또는 다수의 데이터 패킷을 전송하기 때문이다. 따라서 네트워크 필터 드라이버(404)는 해당 응용 프로그램(144)이 스트리밍 서버(122a)에 데이터 전송을 요청한 프로세스에 의해서 수신받은 데이터 패킷인지를 구분하여 응용 프로그램으로 전달해 주어야 하며, 네트워크로부터 데이터 패킷이 전달되기를 기다리는 프로그램을 잠시 중지시키거나 활성화시키고, 모든 라우팅과 주소 분석에 관한 작업도 수행해 주어야 한다.

이러한 네트워크를 통해 송수신하는 수많은 데이터를 처리하기 위하여 이벤트 핸들러(event handler)를 사용하게 된다. 이벤트 핸들러라고 하는 것은 하드웨어 장치에 어떤 특별한 사건이 발생했을 때에 호출되어 작업을 수행하는 일종의 포인터 함수 프로그램을 가리킨다. 네트워크 장치에서 이벤트 핸들러의 값이 만약 0이라면 네트워크 연결을 끊으라는 것을 의미하며, 0이 아닌 임의의 값을 가지면 네트워크 를 통해서 특정 프로세스가 진행된다는 것을 의미하게 된다.

이와 같이 네트워크 드라이버(403)는 응용프로그램(144)과 연결되어 네트워크를 통한 데이터의 수신(receive), 전송(send), 연결(connect), 연결끊음(disconnect) 등의 기능을 수행하게 된다. 본 발명에서는 네트워크 드라이버(403)의 응용프로그램(144) 방향으로 상단에 네트워크 필터 드라이버(404)를 별도로 제작하여 삽입시킴으로써, 응용프로그램(144)과 네트워크 드라이버(403) 사이에서 메시지와 데이터 패킷의 후킹 및 변경, 복호화, 전달하는 필터링 작업을 수행하게 된다.

도 7은 응용 프로그램이 네트워크 연결을 이루기 위한 준비과정을 보여주는 흐름도를 보여준다.

일반적으로 클라이언트 시스템(140)의 사용자(401)가 콘텐트 제공자의 웹페이지에 게시되어 있는 스트리밍 방식으로 서비스되는 콘텐트를 선택하여 클릭하면, DRM 제어기(141)가 DRM 서버(130)로부터 전달받은 정보를 이용해 각종 인증과정을 수행한 후, 해당 응용 프로그램(144)을 실행시키고 잠시 중지시킨다.

그 후 DRM 제어기(141)는 네트워크 필터 드라이버(404)의 초기화를 수행하고 난 후, 이 네트워크 필터 드라이버(404)의 전역변수(global variable)로서 프로세스 아이디를 등록시키고, 복호화키 값을 넘겨주고서 다시 응용프로그램(144)을 활성화시킨다.

그러면 응용프로그램(144)은 외부의 스트리밍 서버(122a)와 연결하기 위한 준비과정의 메시지를 네트워크 드라이버(403)에 전달하게 된다. 이 때 네트워크 필터 드라이버(404)는 응용프로그램(144)에서 네트워크 드라이버(403)에 전달하는 메시지를 후킹하게 된다. 다음으로 이렇게 후킹된 메시지에 의하여, 먼저 네트워크의 연결여부를 확인하는 핸들러가 0인지를 확인하는 과정(702)을 거친다.

만약 핸들러가 0이라면 네트워크 연결을 끊으라는 의미이므로 등록되어 있는 어드레스 핸들(address handle)을 삭제(705)하고서, 네트워크 드라이버(403)로 메시지를 전달하게 된다. 만약 핸들러가 0이 아니면 네트워크와 연결하겠다는 메시지이므로 상기 응용 프로그램(144)의 프로세스 아이디(Process ID)가 네트워크 필터 드라이버(404)에 등록되어 있는지를 확인(703)한다.

만약 프로세스 아이디가 등록되어 있지 않는 것이라면 다른 응용 프로그램이 네트워크 드라이버를 호출하는 것을 의미하므로 그대로 통과시켜 네트워크 드라이버(403)로 메시지를 전달하게 된다. 그러나 만약 프로세스 아이디가 네트워크 필터 드라이버(404)의 초기화의 수행 후 등록된 프로세스라면 새롭게 네트워크의 주소를 구별하고 필터링하기 위한 어드레스 핸들(address handle)의 등록 및 마이이벤트 핸들러(MyEventHandler)의 설정, 로컬포트의 저장을 해주는 작업(704)을 수행하고 난 뒤, 네트워크 드라이버(403)로 변경된 메시지를 전달하게 된다.

여기서 어드레스 핸들의 등록은 다른 응용 프로그램과의 네트워크 주소를 구분하여 제어할 수 있는 어드레스 핸들을 지정하는 과정이 되며, 마이이벤트 핸들러의 설정은 네트워크를 통해 수신된 암호화된 콘텐트 데이터를 복호화하는 작업을 수행하기 위해 별도의 이벤트를 만들어 주는 것이다. 또한 로컬포트를 저장하는 것은 외부 스트리밍 서버(122a)와 네트워크망을 통해 통신할 수 있는 클라이언트 시스템(140)의 로컬포트를 지정해 주는 것이다.

이후 네트워크 드라이버(403)는 응용프로그램(144)에게 외부의 스트리밍 서버(122a)와의 연결을 위한 준비를 완료했다는 메시지를 전달하게 된다.

도 8은 응용 프로그램이 네트워크 연결을 이루는 과정을 보여주는 흐름도이다.

상술한 바와 같이 응용프로그램(144)이 네트워크 연결을 이루기 위한 준비과정을 마쳤다는 메시지를 네트워크 드라이버(403)로부터 받게 되면, 네트워크 필터 드라이버(404)는 응용프로그램(144)이 네트워크 드라이버(403)로 전송하는 메시지를 또 한번 후킹하여 다시 프로세스 등록 여부를 확인(801)한다. 그 후 외부 스트리밍 서버(122a)의 리모트 포트(Remote Port 또는 Server Port)가 미리 정해져 있는 번호, 예컨대 1755인지를 확인(802)한다.

만약 리모트 포트가 1755라면 윈도미디어서버를 사용하는 스트리밍 서버(122a)라는 의미이므로 리모트 포트 1755에 연결된 로컬 포트를 가진 어드레스핸들 구조체(Address Handle Structure)에 리모트포트 1755를 저장(803)하고 난 뒤, 네트워크 드라이버(403)로 메시지를 전달하게 된다. 그리고 추가적으로 어드레스 핸들 구조체는 원래 네트워크 필터 드라이버(404)가 후킹을 통해 변경되지 않은 오리지널 핸들러와 변경된 핸들러, 로컬포트 및 리모트포트의 정보를 저장하게 된다.

참고로, 각각의 프로토콜은 특정한 리모트 포트의 번호를 사용하고 있으며, 예를 들어 포트번호가 21이라면 FTP(File Transfer Protocol)을 사용하는 것을 의미하고, 80번이라면 World Wide Web HTTP를 사용하는 것을 의미하며, 110번이라면 Post Office Protocol Version 3을 의미하고, 1755번이면 윈도미디어서버의 MMS(Microsoft Windows Media Server) 프로토콜을 사용하는 것을 의미하게 된다. 따라서 본 발명에서 리모트 포트가 1755인 것을 확인하는 것은 단순히 윈도미디어서버의 MMS 프로토콜을 사용하는 것을 실시예로서 쉽게 설명하기 위한 것이며, 다른

프로토콜을 이용하여 스트리밍 서비스를 하는 것에 대해 적용한다면 1755번호 대신에 해당 리모트 포트의 번호를 확인하는 과정을 거치면 된다.
도 9는 스트리밍 방식으로 수신한 데이터의 복호화 과정을 보여주는 흐름도이다.
상술한 네트워크 연결과정이 끝나고 나면 본격적으로 네트워크 드라이버(403)는 외부의 스트리밍 서버(122a)와 연결되어 스트리밍 방식으로 암호화된 콘텐트 패키지(142)의 데이터를 수신(901)하게 된다. 상기 수신된 암호화된 패키지의 데이터는 네트워크 드라이버(403)로 전달되게 되며, 네트워크 연결을 준비하는 과정을 통해 미리 설정해 놓았던 마이이벤트 핸들러가 활성화된다. 상기 핸들러가 활성화되면 네트워크 드라이버(403)를 통해 수신된 데이터(142)의 리모트 포트가 1755포트라는 것을 다시 확인(902)한다.
만약 리모트 포트가 1755가 아니라면 다른 응용 프로그램이 요청한 데이터이므로 그냥 통과시킨다. 그러나 만약 리모트 포트가 1755라면 본 발명에서의 해당 응용 프로그램(144)이 요청한 데이터가 수신된 것을 의미하게 된다.
다음 과정으로는 반드시 필요한 필수 과정은 아니지만, 일 실시예에 의하면 하드 디스크에 저장할지의 여부를 확인(903)하게 된다.
만약 저장하라는 것이면, 하드 디스크의 임시 디렉토리에 암호화된 콘텐트 데이터(142)를 저장하고(904) 복호화 과정(905)으로 넘기게 된다. 만약 하드 디스크에 저장하지 않아도 되는 콘텐트 데이터라면, 그대로 복호화 과정(905)으로 전달 하게 된다.
상기 복호화 과정은 DRM 제어기(141)가 DRM 서버(130)로부터 인증과정 후에 전달받은 복호화키(143a)를 네트워크 필터 드라이버(404)에 전역함수로서 미리 등록해 놓은 것을 이용하며, 암호화할 때와 반대과정을 통한 블록암호화 알고리즘을 사용하여 복호화를 수행한다.
이렇게 복호화된 데이터를 응용프로그램(144)에 전달시키게 된다.
그런데, 상기 복호화 과정에서는 상술한 바와 같이 외부의 스트리밍 서버(122a)에서 암호화하지 않은 제어 정보와 암호화된 콘텐트 데이터를 동시에 전송받은 것을 복호화하는 것이므로, 암호화되지 않은 제어 정보는 그대로 응용 프로그램(144)으로 전달하고, 암호화된 콘텐트 데이터는 복호화를 수행하고 난 후 응용 프로그램(144)에 전달하게 된다.
또한 본 발명에서는 콘텐트 데이터를 전부 암호화하는 것을 기본적으로 가정하고 있으나, 암호화와 복호화의 효율성을 높이기 위해 콘텐트 데이터를 전부 암호화하지 않고 부분적으로만 암호화하는 방법을 취할 수도 있음을 밝혀 둔다. 따라서 콘텐트 데이터가 전부 암호화된 것이라면 콘텐트 데이터 부분만을 찾아서 복호화를 수행해 주고, 만약 특정 소리 또는 영상의 부분적 키 프레임만을 암호화한 것이라면 해당 암호화된 키 프레임의 콘텐트 데이터를 찾아서 복호화해 주게 된다.
이렇게 스트리밍 방식으로 전달되는 콘텐트 데이터의 일부분만 암호화하는 이유는 엔코딩 및 디코딩의 효율성을 높이기 위한 것으로서, 그 암호화될 부분과 남겨질 부분은 미리 암호화할 때 정해 주어야 하며, 이에 대한 정보는 파일헤더에 삽입하여 쉽게 클라이언트 시스템(140)에 전달할 수 있다.
한편, 암호화된 콘텐트 데이터(142)를 하드디스크의 임시 디렉토리에 저장하는 기능을 활성화시켜 놓으면 사용자(401)가 스트리밍 방식으로 콘텐트를 모두 보는 동안 자신의 하드디스크에 암호화된 콘텐트를 저장하여, 그 후에 재사용할 수 있게끔 지원할 수도 있다. 이러한 스트리밍 콘텐트의 동시저장 기능은 콘텐트 제공자가 임의로 설정할 수 있으며, 이때 사용자(401)는 재사용성이 높은 온라인교육 콘텐트와 같은 것을 암호화된 상태로 자신의 하드디스크에 저장시켜 놓고 나중에 다시 사용할 수 있지만, 다른 클라이언트 시스템으로 불법복제 또는 무단배포를 한다고 하여도 암호화되어 있는 상태이므로 안전하게 저작권을 보호할 수 있게 된다.
이때 다른 클라이언트 시스템으로 전달된 암호화된 콘텐트가 DRM 서버(130)의 정보를 가지고 새로운 인증을 받거나 또는 사용권한을 포함한 상태의 암호화된 콘텐트 패키지(142)가 다른 사용자에게 전달될 수 있도록 설정해 놓으면, 사용자간의 슈퍼배포(superdistribution)를 통한 콘텐트 판매의 증가를 지원하게 된다.
이제 스트리밍 서비스와 데이터의 전송 포맷에 대하여 고찰한다.
스트리밍 방식으로 서비스되는 멀티미디어 파일 포맷 중에 현재 세계적으로 가장 많이 사용되고 있는 대표적인 것이 ASF(Advanced Streaming Format)이다. ASF는 마이크로소프트가 개발한 멀티미디어 콘텐트의 송수신 데이터 포맷이며, 멀티미디어 데이터 등을 분할하고 그것을 포함한 패킷의 사양을 규정하고 있다. 상기 ASF는 멀티미디어 압축 등의 포맷을 정한 것이 아니라, AVI(Audio Video Interleaved의 포맷)나 MOV(QuickTime 플레이어의 데이터 포맷), MPG(Moving Picture Experts Group 의 포맷) 등의 멀티미디어 데이터를 주고받기 위한 구조이며, 리얼네트웍스의 리얼비디오 파일 포맷도 ASF에 포함된 형태로 송수신되게 된다.
이러한 하나의 ASF 파일은 여러 개의 오브젝트(Object) 단위로 구성되어 있으며, 크게 헤더 오브젝트(Header Object), 데이터 오브젝트(Data Object), 인덱스 오브젝트(Index Object) 및 기타 오브젝트(Other Objects)로 구성되어 있다.
상기 헤더 오브젝트는 파일특성 오브젝트(File Properties Object), 다수의 스트림 특성 오브젝트(Stream Properties Object), 기타 헤더오브젝트(Other Header Object) 등으로 구성되어 있다. 또한 각각의 오브젝트는 16바이트의 오브젝트 아이디(Object ID), 8바이트의 오브젝트 크기(Object Size), 임의의 크기인 오브젝트 데이터(Object Data)로 구성된다.
또한 ASF 포맷은 재생 타이밍 조정과 동기도 자유롭게 구현할 수 있으며, 하위층의 프로토콜을 선택하지 않는 것이 특징이다. 클라이언트에서 데이터 송신요구가 있으면 우선 서버는 멀티캐스트 IP, UDP, RTP, TCP, HTTP의 순서로 테스트하여 이용 가능한 가장 좋은 효율의 프로토콜을 자동으로 선택해 준다. 최악의 경우 웹을 통해 볼 수 있는 환경만 되면 특별한 설정변경 없이 멀티미디어 콘텐트의 스트리밍 재생을 볼 수 있게 해 준다.
또한 MMS(Microsoft Windows Media Server) 프로토콜은 멀티미디어 파일을 스트리밍하는데 사용하는데 가장 많이 사용하는 프로토콜로서, 마이크로소프트 인터넷 익스플로러 등의 웹 브라우저와 연동되어 있으며, 또한 윈도 미디

어 플레이어와도 연동되어 최적의 스트리밍을 지원하도록 설계되어 있다. MMS 프로토콜은 인터넷 기본 프로토콜인 HTTP 프로토콜보다 보안이 높고 안정적으로 스트리밍 서비스가 가능한 미디어 서버용 프로토콜로서, 사용자의 전송 요구가 발생할 경우 기존 HTTP, UDP, TCP 3가지 방식의 프로토콜 중에서 가장 적합한 프로토콜을 선택해 최적의 스트리밍을 구현하는 방식을 사용하게 된다.

도 10은 멀티미디어 스트리밍 콘텐트의 파일 형식을 보여주는 모식도이다.

상술한 바와 같이 ASF 파일 포맷에는 헤더 오브젝트, 데이터 오브젝트, 인덱스 오브젝트, 기타 오브젝트로 구성되어 있다.

본 발명에서의 스트리밍 콘텐트를 암호화하기 위해서는 헤더 오브젝트 내의 확장 콘텐트 묘사 오브젝트(Extended Content Description Object)에 DRM 패키지 헤더를 삽입하는 것이 바람직하다. 그리고 스트리밍 방식의 콘텐트를 암호화하기 위해서는 응용 프로그램과 외부의 스트리밍 서버가 통신하는 제어 정보의 하나인 헤더 오브젝트는 암호화하지 않고 데이터 오브젝트만을 암호화하는 것이 효율적이게 된다. 왜냐하면 본 발명의 중요한 특징 중의 하나인 기존의 스트리밍 방식으로 콘텐트를 서비스하기 위한 프로토콜과 서버의 구조변경 없이 암호화한 콘텐트를 스트리밍 방식으로 전송하기 위해서는 데이터 오브젝트만을 암호화해서 네트워크 필터 드라이버에서 복호화하여 해당 응용 프로그램으로 전달해 주기 위해서이다.

이때 데이터 오브젝트는 전부 암호화할 수도 있으며, 암호화 및 복호화의 효율성을 높이기 위해 특별한 프레임만 선택하여 부분적 암호화 및 복호화를 수행할 수도 있다. ASF의 데이터 오브젝트는 여러 개의 데이터 유니트들로 구성되어 있으며, 하나의 멀티미디어 세그먼트 내에는 소리 및 영상파일들의 프레임이 포함되어 있다.

따라서 데이터 오브젝트의 부분 암호화를 위해서는 소리 또는 영상의 키(key) 프레임만을 찾아서 암호화 및 복호화해주는 기능을 구현하였다. 소리와 영상의 키 프레임은 각각 위치를 표시하는 특별한 인식기호를 가지고 있으므로 프로그램적으로 쉽게 해당 위치를 찾아 암호화 및 복호화시킬 수 있다. 이때 데이터 오브젝트의 전부 암호화 또는 부분 암호화하는 방식에 대한 정보는 DRM 패키지 헤더에 표시해 줌으로써 복호화할 때 활용할 수 있는 정보를 제공해 주게 된다.

만약 소리는 암호화하지 않고 영상만 암호화하게 되면 정당한 사용권한을 획득하지 못한 사용자의 경우 소리는 정상적으로 들리지만, 화면은 깨져서 나오는 유선방송이나 셋톱박스에서의 스크램블 효과를 얻을 수도 있게 된다.

도 11은 DRM 패키지의 헤더 형식을 보여주는 모식도이다.

상술한 스트리밍 콘텐트의 암호화한 패키지를 제작할 때 임의로 제작하여 삽입하는 DRM 패키지 헤더에는 패키지의 버전번호(version number), 콘텐트 URI 길이(content URI length), 콘텐트타입 길이(content type length), 콘텐트 URI(content URI), 콘텐트 타입(content type), 헤더 길이(header length), 데이터 길이(data length), 암호화 방법(encryption method), 권리 발행자 URL(rights issuer URL), 콘텐트 이름(Content name), 콘텐트 설명(content description), 콘텐트 벤더(content vendor), 아이콘 URI(icon URI), 디지털 서명(digital signature), 콘텐트 서버 URL(content server URL) 등의 정보로 구성할 수 있다. 이러한 DRM 패키지 헤더의 형식을 통일시켜 주면 스트리밍 방식이나 다운로드 방식에서 일관된 콘텐트의 서비스가 가능하게 된다. 또한 유무선 인터넷을 활용하여 PC 또는 노트북, PDA, 휴대폰, 셋톱박스, 디지털TV, 텔레메틱스 단말기 등의 다양한 클라이언트 시스템에서 DRM을 적용한 콘텐트의 통합된 유통을 지원할 수 있게 된다.

상기 DRM 패키지 헤더에는 콘텐트 정보, 암호화방법, 라이센스 발급기의 위치, 전자서명, 콘텐트 서버 등의 각종 DRM 서비스를 위해 필요한 정보들을 규정하고 있다. 여기서 URI(Uniform Resource Identifier, 통일 리소스 식별자)를 의미하며, URI를 이용하면 액세스 방법이 다른 다양한 유형의 리소스 정보를 동일한 식별기호를 이용해 처리할 수 있게 된다.

상기 설명은 VOD 스트리밍 뿐만 아니라 라이브 스트리밍에도 매우 유사하게 적용될 수 있다.

즉, 상술한 설명에는 주로 이미 만들어져 있는 멀티미디어 콘텐트를 암호화하여 스트리밍 서버에 올리는 방식으로 서비스되는 VOD(Video On Demand)에 대해 자세히 설명되어 있으나, 본 발명에서 설명한 기술을 이용하여 스포츠 또는 뉴스, 공연 등의 라이브 스트리밍을 지원하는 DRM 시스템을 구현할 수도 있다.

일반적인 라이브 스트리밍은 실시간 중계를 하는 카메라와 마이크에서 송출된 영상 및 소리의 데이터를 멀티미디어로 엔코딩하여 스트리밍 서버로 전송시킨 후, 유무선 인터넷을 통해 클라이언트 시스템의 사용자에게 서비스하게 된다. 따라서 도 1에서 설명한 암호화를 담당하는 콘텐트 패키저 프로그램의 콘텐트 소스로서 마이크와 카메라와 멀티미디어 엔코딩 시스템에 연결시키면 엔코딩되어 실시간으로 유입되는 멀티미디어 콘텐트 데이터를 스트리밍 서버로 전송하기 전에 암호화할 수 있다.

이때 콘텐트 패키저에서의 암호화는 라이브 스트리밍의 엔코딩 시스템의 TDI 드라이버 상단에 네트워크 필터 드라이버에서 이루어지는 것이 바람직하다. 따라서 상술한 바와 같은 클라이언트 시스템이 전송받은 암호화된 데이터의 네트워크 필터 드라이버에서의 후킹과 복호화하는 기술을 콘텐트제공 시스템에도 적용할 수 있다. 즉, 멀티미디어 콘텐트의 라이브 스트리밍을 위한 엔코딩 시스템에서 엔코딩된 콘텐트를 외부의 스트리밍 서버로 송신하기 직전에 네트워크 필터드라이버가 원본 데이터를 후킹하여 실시간으로 암호화해 주면 된다. 이때 사용하는 암호화 알고리즘이나 암호화 방법, 복호화 방법 등은 상술한 VOD 스트리밍과 같은 방식으로 아무런 변형 없이 이용할 수 있다.

그러나 최근 들어 라이브 스트리밍의 높은 전송 효율을 위해 많이 사용하는 멀티캐스팅을 지원하는 DRM 시스템을 구현하기 위해서는 클라이언트 시스템에서 TCP 프로토콜 대신에 UDP 프로토콜을 이용할 수 있게끔 맞추어 주어야 한다. 즉 UDP는 TCP와 달리 네트워크 전송과정 중에 데이터의 오류가 발생할 수 있으므로, 클라이언트 시스템의 네트워크 필터 드라이버는 복호화할 때 만약 UDP를 사용하여 수신받은 것이라면 손실된 데이터를 수정해 주고서 복호화할 수 있는 기능을 추가적으로 더 구비하여야 한다.

도 12의 A-E는 클라이언트 시스템의 다양한 운영체제에서의 DRM 제어기의 위치를 보여주는 모식도이다. 상기 모식도는 간략하게 운영체제를 도시한 것이기 때문에 각 운영체제의 업그레이드나 새로운 운영체제의 개발에 따라 세밀한 부분에서는 약 간의 차이가 생길 수 있을 수 있으나, 당업자라면 본 발명의 기술적 사상을 그대로 쉽게 적용할 수 있을 것이다.

도 12A는 마이크로소프트의 윈도우 운영체제를 보여주는 모식도이다. 사용자 모드에는 응용프로그램(applications)과 Win32 API(Application Programming Interface)가 있고, 커널모드에는 크게 네트워크 드라이버와 파일시스템 드라이버, 그 외에 그래픽 드라이버(graphics driver), 보안 매니저(security manager), 프로세스 매니저(process manager), 가상메모리(virtual memory), HAL(Hardware Abstraction Layer) 등의 장치가 있고 각각의 디바이스를 구동할 수 있는 디바이스 드라이버가 존재한다. 본 발명에서 멀티미디어 스트리밍 콘텐트의 정보보호를 위한 네트워크 필터 드라이버는 네트워크 필터 드라이버인 TDI 드라이버 상단에 위치시킬 수 있다. 또한 본원 발명의 출원인이 이미 출원한 기술에 해당하는 클라이언트 시스템에 다운로드 또는 저장되어 있는 암호화된 콘텐트를 플레이하기 위한 파일 필터 드라이버는 파일시스템 드라이버(file system driver)의 상단에 위치시키면 된다.

도 12B는 마이크로소프트의 WinCE 운영체제를 보여주는 모식도이다. 마이크로소프트의 WinCE는 보통 PC보다 하드웨어 사양이 떨어지는 PDA나 셋톱박스의 운영체제로 많이 사용되고 있다. 윈도우 운영체제와 마찬가지로 네트워크 필터 드라이버는 네트워크 드라이버의 상단에 위치시킬 수 있고, 파일 필터 드라이버는 파일시스템 드라이버의 상단에 위치시킬 수 있다. 본 모식도에서 Win32 API Thunk는 16비트와 32비트의 메모리 주소를 상호 변환해 주는 역할을 수행하는 것이며, GWES(Graphics, Windowing and Event Subsystem)는 사용자 모드와 GDI(Graphic Device Interface) 콤포넌트를 하나의 서브시스템으로 통합시킨 것이다. 또한 쓰레드(thread)는 프로세스의 내부 수행경로를 의미하는 것이며, 스케쥴링(scheduling)은 일련의 작업에 걸리는 시간의 견적과 그 진척사항을 관리하는 기능을 의미하고, 윈속(winsock)은 인터넷 접속 프로그램이며, FSD(FileSystem Drier) 매니저는 파일시스템 드라이버를 관리하는 프로그램이다.

도 12C는 리눅스 운영체제를 보여주는 모식도이다. 리눅스 운영체제는 완전 무료로 공개된 유닉스 호환 운영체제이며, 윈도우 운영체제와 크게 다르지는 않다. 여기서 네트워크 필터 드라이버는 네트워크 드라이버 상단에 위치시킬 수 있으며, 파일 필터 드라이버는 저장장치를 관리하는 파일시스템과 유사한 블록 디바이스(block device)쪽에 위치시킬 수 있다. 블록 디바이스는 리눅스에서 데이터를 하드디스크 또는 플래시메모리, CD롬 같은 저장장치를 어떻게 관리해야 하는지 관장하는 것 드라이버이다.

도 12D는 팜 운영체제를 보여주는 모식도이며, 팜 운영체제는 PDA 운영체제로 많이 사용되고 있다. 팜(Palm) 운영체제에 대한 자세한 내부 구조는 잘 공개되어 있지 않지만, 윈도우 운영체제와 유사하게 네트워크 필터 드라이버 또는 파일 필터 드라이버를 위치시키기 위해서는 핵마스터(HackMaster)라는 프로그램을 설치하고 그 위에 스트리밍과 다운로드를 지원하는 DRM 제어기를 위치시킬 수 있다.

도 12E는 일반 휴대폰의 운영체제를 보여주는 모식도이다. 휴대폰 운영체제의 커널 모드에는 플랫폼 코어(platform core)가 있고 스트리밍과 다운로드를 지원하는 DRM 제어기는 이곳에 위치시킬 수 있다. 여기서 설명하지 않은 많은 운영체제들도 있으나 원리적인 측면에서는 거의 대등소이하며, 서로 통합 또는 분리 발전하는 경향을 보이고 있으며, 본 발명의 기술적 사상을 상술한 운영체제를 포함한 새로운 운영체제에 적용하는 것은 당업자라면 쉽게 구현할 수 있을 것이다.

도 13은 본 발명에서 암호화를 수행하는 콘텐트 패키저 프로그램의 화면 이미지이다. 상술한 바와 같이 콘텐트 패키저(112)는 DRM 서버 콤포넌트(132)와 통신하여 암호화키를 전달받고 원본 콘텐트를 암호화하게 된다. 이때 암호화는 파일 단위 또는 여러 파일을 포함하고 있는 디렉토리 단위로 암호화를 수행할 수 있으며, 콘텐트 추가, 콘텐트 삭제, 암호화, 콘텐트 서버(122)로의 업로드 등의 아이콘을 구비할 수 있다. 또한 파일, 라이브, 보기, 옵션, 도움말 등의 메뉴를 가지고 있으며, 이러한 메뉴를 통해 암호화할 때 필요한 각종 설정 사항들을 규정할 수 있다.

도 14는 본 발명에서 DRM 관리기 프로그램의 화면 이미지이다. DRM 관리기(134)는 회원의 아이디, 이름, 주민등록번호, 연락처 등의 회원정보, 각 콘텐트의 보안레벨을 설정하는 기능, 각 콘텐트를 서비스하는 사이트를 관리하는 기능, 라이센스의 관리 기능, 사용자 PC의 하드웨어 정보의 관리, 각 로그 통계 분석 기능 등의 메뉴로 구성되어 있다.

도 15는 본 발명에서 암호화된 VOD 스트리밍 콘텐트를 복호화하여 기존의 응용 프로그램으로 보여주는 화면캡처의 이미지이다. 본 화면 이미지는 클라이언트 시스템(140)에 다운로드 또는 저장되어 있는 콘텐트를 플레이하는 것이 아니라, 인터넷으로 연결되어 있는 외부의 스트리밍 서버(122a)로부터 VOD 스트리밍 서비스 방식으로 암호화된 콘텐트 패키지(142)를 수신하고, 이것을 네트워크 필터 드라이버(404)가 복호화하여 기존의 응용 프로그램(144)인 윈도우 미디어 플레이어에서 보여주는 것이다. 따라서 다른 DRM 시스템에서 상용화할 때 가장 문제가 되었던 전용 뷰어 프로그램을 설치하지 않고 기존 응용 프르그램을 이용하여 암호화된 스트리밍 콘텐트를 보여주는 것을 분명하게 확인할 수 있다.

도 16은 본 발명에서 암호화된 VOD 스트리밍 콘텐트를 복호화하여 OCX 플레이어로 보여주는 화면캡처의 이미지이다. 이러한 OCX 플레이어는 최근 인터넷 영화관이나 온라인 교육업체 등에서 많이 사용하고 있는 플레이어로서, 전용 뷰어 프로그램이 아니라 각각의 멀티미디어 콘텐트를 볼 수 있는 미디어 플레이어의 콤포넌트를 익스플로러 또는 넷스케이프와 같은 인터넷 브라우저 프로그램에 플러그인 형태로 삽입하여 다양한 디자인의 스킨과 여러 가지 추가 기능을 구비하도록 만든 것이다. 본 화면 이미지도 상술한 바와 같이 VOD 스트리밍으로 서비스되는 멀티미디어 콘텐트를 네트워크 필터 드라이버(404)가 암호화된 멀티미디어 콘텐트 데이터를 후킹하여 복호화하고, OCX 플레이어에 삽입되어 있는 응용 프로그램 콤포넌트에 복호화된 데이터를 전달하기 때문에 정상적으로 플레이하는 것을 볼 수 있다.

도 17은 본 발명에서 암호화된 라이브 스트리밍 콘텐트를 복호화하여 OCX 플레이어로 보여주는 화면캡처의 이미지이다. 라이브 스트리밍 서비스를 하기 위해서 본원 발명의 출원인 사무실에 디지털 비디오 카메라를 설치하고 디지털 카메라로부터 출력되는 영상과 음성 데이터를 마이크로소프트 엔코딩 서버를 이용해 엔코딩 한 후, 본 발명에서의 콘텐트 패키저가 실시간으로 엔코딩된 영상과 음성 데이터를 엔코딩 시스템의 네트워크 필터 드라이버에서 실시간으로 데이터를 후킹 및 암호화하여 스트리밍 서버(122a)인 마이크로소프트 미디어 서버에 올리게 된다. 이후 클라이언트 시스템(140)은 스트리밍 서버로부터 수신된 암호화된 콘텐트 패키지를 네트워크 필터 드라이버에서 후킹 및 복호화하여 OCX 플레이어를 통해 보여주게 된다.
도 18은 본 발명에서 복호화되지 않은 콘텐트를 플레이할 때 화면캡처의 이미지이다. 본 화면 이미지는 윈도우 미디어 플레이어가 외부의 스트리밍 서버(122a)로부터 암호화된 콘텐트 패키지(142)를 수신받지만, 제대로 된 인증과정을 거치지 않았기 때문에 복호화되지 않고 깨진 상태로 플레이되는 것을 보여주는 것이다. 이때 상술한 바와 같이 스트리밍 멀티미디어 콘텐트의 전체 또는 부분적으로 암호화함으로써 암호화 수준의 조정에 따라 완전히 화면이 나오지 않게 하거나, 소리와 함께 적당하게 깨진 화면을 볼 수도 있다. 이렇게 암호화 수준을 조정함에 따라 일반적인 케이블 방송이나 위성 방송 등에서처럼 스크램블링(scrambling) 기능을 수행할 수도 있다.
이상에서 설명한 본 발명은, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 당업자가 본 발명의 기술적 사상을 벗어나지 않는 범위에서 여러 가지로 치환, 변형 또는 변경이 가능하므로 상술한 일 실시예 및 첨부된 도면에 한정되는 것은 아니다.

발명의 효과

본 발명에서 제안한 커널 모드 제어를 이용한 디지털 콘텐트의 정보보호 방법 및 시스템은 네트워크 필터 드라이버 단계에서의 메시지와 데이터 패킷의 후킹 및 변경, 복호화, 전달하는 필터링 기술을 구현함으로써, 유무선 인터넷을 통해 스트리밍 방식으로 전달되는 다양한 암호화된 콘텐트를 복호화 수단을 구비한 전용 뷰어 프로그램의 개발 없이 기존의 응용프로그램을 사용하여 사용할 수 있는 구체적인 방법을 제공해 주고 있다.
또한 본 발명에서 개시하고 있는 네트워크 필터 드라이버의 아이디어를 활용하면 유무선 인터넷과 네트워크 망을 통해 암호화된 콘텐트를 제공받아 사용하기 위한 PC, 노트북, PDA, 휴대폰, 셋톱박스 등의 클라이언트 시스템의 네트워크 장치에 소프트웨어 또는 추가적으로 간단한 하드웨어 칩을 구비함으로써 불법복제의 위험성을 제거한 상태에서 안전하게 콘텐트를 유통할 수 있는 유무선 통합 DRM 시스템을 구축하는 방법을 제공해 주고 있다.
물론 본 발명의 실시예에서 설명한 응용프로그램은 윈도미디어플레이어에 한정된 것이 아니며, 리얼플레이어 및 퀵타임플레이어, 윈앰프 등 이미 상용화되어 있거나 앞으로 개발될 미디어 플레이어에 쉽게 적용될 수 있다는 것은 자명한 사실이다.
또한 본 발명은 기존의 스트리밍 방식으로 콘텐트를 서비스하는 시스템에 DRM 시스템을 적용함에 따른 추가적인 서버 및 네트워크의 과부하없이 기존의 파일포맷과 프로토콜을 그대로 활용하는 구체적인 방법을 제공해 주고 있다.
뿐만 아니라 본 발명은 현재 상용화되어 있는 거의 모든 콘텐트 파일 형식과 새롭 게 개발되는 새로운 파일 형식에 손쉽게 활용할 수 있으며, 스트리밍을 지원하는 네트워크 필터 드라이버와 다운로드를 지원하는 파일 필터 드라이버를 구현함으로써 스트리밍 및 다운로드를 동시에 지원할 수 있는 DRM 시스템을 구축하는 방법을 제공해 주고 있다.
게다가 네트워크 필터 드라이버 단계에서의 메시지와 데이터 패킷의 후킹과 변경과 같은 필터링 기능을 이용하여 불법적으로 PC의 보안 또는 허가되지 않은 네트워크의 사용을 미연에 방지하는 방화벽 기능의 프로그램을 개발하는 방법을 제공해 주고 있다. 주지되는 바와 같이 본 발명은 실시예에서 자세히 설명한 윈도 운영체제에 국한되는 것이 아니며, 윈도우의 다른 버전, 리눅스, 유닉스, 팜(Palm) OS, 휴대폰 OS 등의 기타 다른 운영체제와 유무선 인터넷을 이용하는 PC, 노트북, PDA, 휴대폰, 셋톱박스 등의 각종 정보처리기기에서도 동일한 기술적 사상 내에서 당업자라면 다양한 변형을 손쉽게 만들어 낼 수 있을 것이다. 또한 본 발명은 컴퓨터 프로그램으로 제작될 수도 있고, 제작된 컴퓨터 프로그램은 기록매체에 저장되거나, 전송매체에 의해 전송될 수도 있다.

(57) 청구의 범위

청구항 1.

각각 CPU, 휘발성 저장장치(메모리), 비휘발성 저장장치(하드디스크), 입출력장치(키보드, 모니터 등)를 가지며, 유무선 내부 통신수단이나 외부 네트워크와의 통신수단에 의하여 연결되어 있는 정보제공 시스템과 클라이언트 시스템으로 구성되며, 상기 클라이언트 시스템은 응용프로그램과 하위 레이어의 드라이버 사이에 위치하여 수신받은 암호화된 데이터를 가로채고, 변경하고, 이를 복호화하여 상기 응용프로그램에 전달하는 필터링 수단을 구비하는, 멀티미디어 스트리밍 콘텐트의 정보보호 시스템에 있어서,
상기 정보제공 시스템은
콘텐트 소스를 암호화하여 콘텐트 패키지(121)를 생성하는 암호화 수단(110)과;
상기 암호화된 콘텐트 패키지(121)를 사용자에게 제공하는 공급 수단(120)과;
암호화키의 생성 관리와 각종 인증을 수행하는 DRM 서버(130)를 포함하고,
상기 클라이언트 시스템은
응용프로그램을 활성화시키고, 상기 필터링 수단을 제어하는 제어수단과;
상기 필터링 수단으로부터 복호화된 콘텐트를 전달받아서 플레이하는 응용프로그램(144)을 포함하되,
상기 필터링 수단이 수신하는 데이터는 외부 네트워크로 연결된 네트워크 드라이버를 통해 수신하며,

상기 멀티미디어 스트리밍 콘텐트는,
라이브/VOD 스트리밍 방식인 것
을 특징으로 하는 멀티미디어 스트리밍 콘텐트의 정보보호 시스템.

청구항 2.
제1항에 있어서, 상기 암호화 수단(110)은 상기 DRM 서버(130)에서 생성시킨 암호화키를 전달받아 콘텐트의 암호화를 수행하는 콘텐트 패키저(112)임을 특징으로 하는 멀티미디어 스트리밍 콘텐트의 정보보호 시스템.

청구항 3.
제1항에 있어서, 상기 공급 수단(120)은 상기 암호화 수단(110)에 의하여 암호화된 콘텐트 패키지(121)가 업로드되는 콘텐트 서버(122)임을 특징으로 하는 멀티미디어 스트리밍 콘텐트의 정보보호 시스템.

청구항 4.
제1항에 있어서, 상기 DRM 서버(130)는
DRM 서버의 각종 콘텐트 정보, 암호화키, 사용자 정보, 응용 프로그램 정보 등을 저장하는 DRM 서버 DB(131)와;
DRM 암호화키의 발생 관리 및 라이센스 발급 관리를 제어하는 DRM 서버 콤포넌트(132)와;
클라이언트 시스템의 DRM 제어기(141)의 요청에 따라 암호화된 라이센스 패키지를 발급하는 DRM 라이센스 발급기(133)와;
DRM 서버의 각종 설정과 관리를 수행하는 DRM 관리기(134);
로 구성됨을 특징으로 하는 멀티미디어 스트리밍 콘텐트의 정보보호 시스템.

청구항 5.
제1항에 있어서, 상기 정보제공 시스템은 유료 서비스시의 비용청구를 위하여 빌링 서버(150) 또는 페이먼트 게이트웨이 서버(160)와의 연계 수단을 더욱 구비함을 특징으로 하는 멀티미디어 스트리밍 콘텐트의 정보보호 시스템.

청구항 6.
제1항에 있어서, 상기 필터링 수단은 상기 제어수단의 지시에 따라 응용프로그램(144)과 외부의 공급 수단(120) 사이의 메시지와 패킷의 후킹 및 변경, 암호화된 콘텐트 패키지(142)의 복호화, 응용 프로그램(144)에 전달하는 필터링 작업을 커널 모드에서 수행하는 네트워크 필터 드라이버(404)임을 특징으로 하는 멀티미디어 스트리밍 콘텐트의 정보보호 시스템.

청구항 7.
제1항에 있어서, 상기 제어 수단은 사용자가 콘텐트를 선택하면 자동으로 활성화되어 응용프로그램(144)을 기동시키고, DRM 서버(130)에 접속하여 콘텐트 및 사용자 인증을 수행한 후 복호화키를 포함한 라이센스 패키지(143)를 수신하며, 응용프로그램(144)의 종료에 따라 필터링 동작을 종료시키며, 상기 필터링 수단을 제어하는 DRM 제어기(141)임을 특징으로 하는 멀티미디어 스트리밍 콘텐트의 정보보호 시스템.

청구항 8.
제1항에 있어서, 상기 응용프로그램(144)은 전용 뷰어 프로그램이 아닌 그 콘텐트 를 플레이할 수 있는 운영체제에 설치되어 있는 일반 응용프로그램임을 특징으로 하는 멀티미디어 스트리밍 콘텐트의 정보보호 시스템.

청구항 9.
제3항에 있어서, 상기 콘텐트 서버(122)는 실제 스트리밍이 제공되는 스트리밍 서버(122a)와, 암호화된 콘텐트를 선택할 수 있는 웹 서버(122b) 또는 FTP 서버로 구성됨을 특징으로 하는 멀티미디어 스트리밍 콘텐트의 정보보호 시스템.

청구항 10.
제6항에 있어서, 상기 네트워크 필터 드라이버(404)는 응용프로그램(144) 방향으로 네트워크 드라이버의 최상단에 위치하는 것을 특징으로 하는 멀티미디어 스트리밍 콘텐트의 정보보호 시스템.

청구항 11.
제10항에 있어서, 상기 네트워크 필터 드라이버(404)는 TCP 프로토콜 또는 부가적으로 수신 데이터의 수정기능을 더욱 구비한 UDP 프로토콜을 사용함을 특징으로 하는 멀티미디어 스트리밍 콘텐트의 정보보호 시스템.

청구항 12.
제1항 내지 제11항 중 어느 한 항에 있어서, 상기 콘텐트는 미리 제작된 원본 콘 텐트임을 특징으로 하는 멀티미디어 스트리밍 콘텐트의 정보보호 시스템.

청구항 13.
제1항 내지 제11항 중 어느 한 항에 있어서, 상기 콘텐트는 미리 제작된 원본 콘텐트가 아니라, 멀티미디어 수신장치와 엔코딩 시스템을 통하여 입력되는 실시간 라이브 콘텐트임을 특징으로 하는 멀티미디어 스트리밍 콘텐트의 정보보호 시스템.

청구항 14.
제13항에 있어서, 상기 실시간 라이브 콘텐트를 외부 스트리밍 서버로 전송하기 이전에 엔코딩 시스템의 네트워크 드라이버 상단에 설치되는 실시간 후킹과 암호화를 위한 네트워크 필터 드라이버를 더욱 구비함을 특징으로 하는 멀티미디어 스트리밍 콘텐트의 정보보호 시스템.

청구항 15.
각각 CPU, 휘발성 저장장치(메모리), 비휘발성 저장장치(하드디스크), 입출력장치(키보드, 모니터 등)를 가지며, 외부 네트워크와의 통신수단에 의하여 연결되어 있는 정보제공 시스템과 클라이언트 시스템을 이용하여 스트리밍되는 라이브/VOD 스트리밍 방식의 멀티미디어 스트리밍 콘텐트의 정보보호 시스템에 있어서,

스트리밍에 의하여 전송되는 암호화된 콘텐트 패키지(142)가 적어도 암호화된 콘텐트(142a)인 데이터 오브젝트 부분과, 암호화되지 않은 메타 데이터(142b)인 헤더 오브젝트 부분으로 구성됨을 특징으로 하는 멀티미디어 스트리밍 콘텐트의 정보보호 시스템.

청구항 16.

제15항에 있어서, 상기 암호화된 콘텐트 패키지(142)의 DRM 패키지 헤더는 멀티미디어 콘텐트 파일포맷의 헤더 오브젝트에 기록됨을 특징으로 하는 멀티미디어 스트리밍 콘텐트의 정보보호 시스템.

청구항 17.

제16항에 있어서, 상기 DRM 패키지 헤더에는 버전 번호, 콘텐트 URI 길이, 콘텐트 타입 길이, 콘텐트 URI, 콘텐트 타입, 헤더 길이, 데이터 길이, 암호화 방법, 권리 발행자 URL, 콘텐트 이름, 콘텐트 설명, 콘텐트 벤더, 아이콘 URI, 디지털 서명, 콘텐트 서버 URL의 정보가 기록됨을 특징으로 하는 멀티미디어 스트리밍 콘텐트의 정보보호 시스템.

청구항 18.

제15항에 있어서, 상기 암호화된 콘텐트(142a) 부분인 데이터 오브젝트는 그 내용의 전부가 암호화되거나 또는 미리 정해진 프레임 단위로 일부만 암호화됨을 특징으로 하는 멀티미디어 스트리밍 콘텐트의 정보보호 시스템.

청구항 19.

제15항에 있어서, 상기 클라이언트 시스템에는 암호화된 콘텐트 패키지(142)를 하드디스크에 저장하는 수단을 더 포함하는 것을 특징으로 하는 멀티미디어 스트리밍 콘텐트의 정보보호 시스템.

청구항 20.

각각 CPU, 휘발성 저장장치(메모리), 비휘발성 저장장치(하드디스크), 입출력장치(키보드, 모니터 등)를 가지며, 외부 네트워크와의 통신수단에 의하여 연결되어 있는 정보제공 시스템과 클라이언트 시스템을 이용하여 스트리밍되는 라이브/VOD 스트리밍 방식의 멀티미디어 스트리밍 콘텐트의 정보보호 시스템에 있어서,
사용자의 인증요청에 따라 클라이언트 시스템으로 전송되는 암호화된 라이센스 패키지(143)가 적어도 암호를 풀기 위한 복호화키(143a) 부분과, 콘텐트의 사용횟수와 사용기간, 단말기 제한 정보를 포함하는 사용권한에 관한 정보(143b) 부분으로 구성됨을 특징으로 하는 멀티미디어 스트리밍 콘텐트의 정보보호 시스템.

청구항 21.

각각 CPU, 휘발성 저장장치(메모리), 비휘발성 저장장치(하드디스크), 입출력장치(키보드, 모니터 등)를 가지며, 외부 네트워크와의 통신수단에 의하여 연결되어 있는 정보제공 시스템과 클라이언트 시스템을 이용하여 스트리밍되는 라이브/VOD 스트리밍 방식의 멀티미디어 스트리밍 콘텐트의 정보보호 방법에 있어서,
콘텐트 소스(111)를 암호화하여 암호화된 콘텐트 패키지(121)로 만들어 콘텐트 서버(122)에 업로드하는 암호화 및 업로드 단계와;
사용자가 웹 서버(122b) 또는 FTP 서버에서 선택함에 의하여 스트리밍 서버(122a)에 클라이언트 시스템을 연결하는 시작 및 연결 단계;
스트리밍되는 콘텐트 데이터를 복호화하면서 응용프로그램(144)을 통하여 플레이하는 복호화 및 플레이 단계;
DRM 제어기(141)가 응용프로그램(144)의 종료 메시지를 감지하여 종료하면서 스트리밍 서버(122a)와의 연결을 해제하는 종료 및 연결해제 단계;
로 구성됨을 특징으로 하는 멀티미디어 스트리밍 콘텐트의 정보보호 방법.

청구항 22.

제21항에 있어서, 상기 암호화 및 업로드 단계는
콘텐트 패키저(112)가 DRM 서버(130)에 인증 요청을 하는 단계(S201)와;
이에 대하여 DRM 서버(130)가 콘텐트 패키저(112)에 인증 결과를 보내는 단계(S202)와;
콘텐트 패키저(112)가 DRM 서버(130)에 암호화키 요청을 하는 단계(S203)와;
이에 대하여 DRM 서버(130)가 콘텐트 패키저(112)에 암호화키를 보내는 단계(S204)와;
상기 암호화키를 이용하여 콘텐트 패키저(112)가 콘텐트를 블록 암호화 알고리즘을 사용하여 암호화하는 단계와;
콘텐트 패키저(112)가 스트리밍 서버(122a)에 인증 요청을 하는 단계(S205)와;
이에 대하여 스트리밍 서버(122a)가 콘텐트 패키저(112)에 인증 결과를 보내는 단계(S206)와;
콘텐트 패키저(112)가 스트리밍 서버(122a)에 암호화된 콘텐트 패키지(121)를 보내는 단계(S207);
로 구성됨을 특징으로 하는 멀티미디어 스트리밍 콘텐트의 정보보호 방법.

청구항 23.

제21항에 있어서, 시작 및 연결 단계, 복호화 및 플레이 단계, 종료 및 연결해제 단계는 순차적으로
사용자의 콘텐트 선택에 의하여 웹 서버(122b) 또는 FTP 서버가 DRM 제어기(141)에 콘텐트 식별정보와 사용자 식별정보를 보내는 단계(S301)와;
DRM 제어기(141)가 DRM 서버(130)에 콘텐트 및 사용자의 인증을 요청하는 단계(S302)와;
DRM 서버(130)가 DRM 제어기(141)에 복호화키 및 사용권한 정보 등 라이센스 인증 내용을 보내는 단계(S303)와;
DRM 제어기(141)가 응용프로그램(144)을 기동시키고, 스트리밍 서버(122a)의 URL을 전달하는 단계(S304)와;
응용프로그램(144)이 스트리밍 서버(122a)에 콘텐트 데이터를 요청하는 단계(S305)와;
DRM 제어기(141)가 응용프로그램(144)의 종료 명령을 검출(S307)할 때까지 스트리밍 서버(122a)가 응용프로그램(144)에 제어정보와 데이터 패킷을 주기적으로 전송하고, 이 데이터 패킷이 네트워크 필터 드라이버(404)에 의하여 복호화되어 플레이되는 단계(S306)와;

DRM 제어기(141)가 응용프로그램(144)의 종료 명령을 검출하면, 응용프로그램(144)을 종료시키고, 스트리밍 서버(122a)와의 연결을 해제시키는 단계;
로 구성됨을 특징으로 하는 멀티미디어 스트리밍 콘텐트의 정보보호 방법.

청구항 24.
제21항 또는 제23항에 있어서, 시작 및 연결 단계는
사용자의 콘텐트 선택에 의하여 응용프로그램(144)의 기동과 핸들러의 검사, 프로세스의 등록을 행하는 연결준비 단계와;
이 후의 프로세스의 등록, 리모트 포트의 확인 및 저장을 행하는 연결 단계로 구성됨을 특징으로 하는 멀티미디어 스트리밍 콘텐트의 정보보호 방법.

청구항 25.
제24항에 있어서, 연결준비 단계는
사용자가 콘텐트를 선택함(701)에 의하여 DRM 제어기(141)가 응용프로그램(144)을 기동시킨 후 일시 정지시키는 단계와;
DRM 제어기(141)가 네트워크 필터 드라이버(404)를 이용하여 응용프로그램(144)과 네트워크 드라이버 사이의 메시지를 후킹하여 핸들러가 0(제로)인지를 판단하는 단계와;
핸들러가 0이면 연결을 단절하기 위하여 어드레스 핸들을 삭제한 후 네트워크 드라이버에 메시지를 전달하고, 핸들러가 0이 아니면 진행하여 다시 네트워크 필터 드라이버(404)에 프로세스가 등록되어 있는지를 판단하는 단계와;
프로세스가 등록되어 있지 않으면 네트워크 드라이버에 그대로 메시지를 전달하고, 프로세스가 등록되어 있으면 어드레스 핸들을 등록하고, 마이이벤트 핸들러를 설정하며, 로컬 포트를 저장한 후에 네트워크 드라이버에 변경된 메시지를 전달하는 단계와;
메시지의 전달에 의하여 응용프로그램(144)이 네트워크 드라이버로부터 준비완료 메시지를 전달받는 단계;
로 구성됨을 특징으로 하는 멀티미디어 스트리밍 콘텐트의 정보보호 방법.

청구항 26.
제24항에 있어서, 연결 단계는
네트워크 필터 드라이버(404)가 응용프로그램(144)과 네트워크 드라이버 사이의 메시지를 후킹하여 네트워크 필터 드라이버(404)에 프로세스가 등록되어 있는지를 판단하는 단계(801)와;
프로세스가 등록되어 있지 않으면 네트워크 드라이버에 그대로 메시지를 전달하 고, 프로세스가 등록되어 있으면 다시 리모트 포트가 미리 정해져 있는 번호인지를 판단하는 단계와;
리모트 포트의 번호가 미리 정해져 있는 번호가 아니면 네트워크 드라이버에 그대로 메시지를 전달하고, 리모트 포트의 번호가 미리 정해져 있는 번호이면 그 리모트 포트에 연결된 로컬 포트를 가진 어드레스 핸들 구조체에 리모트 포트 번호를 저장한 후 네트워크 드라이버에 그대로 메시지를 전달하는 단계;
로 구성됨을 특징으로 하는 멀티미디어 스트리밍 콘텐트의 정보보호 방법.

청구항 27.
제21항 또는 제23항에 있어서, 복호화 및 플레이 단계는
네트워크 드라이버가 네트워크를 통하여 스트리밍 방식으로 데이터를 수신하는 단계(901)와;
마이이벤트 핸들러가 활성화되어 리모트 포트가 미리 정해져 있는 번호인지를 판단하는 단계와;
리모트 포트가 미리 정해져 있는 번호가 아니면 응용프로그램(144)에 데이터를 그대로 전송하고, 리모트 포트가 미리 정해져 있는 번호이면 응용프로그램(144)에 데이터를 복호화(905)한 후에 전송하는 단계;
로 구성됨을 특징으로 하는 멀티미디어 스트리밍 콘텐트의 정보보호 방법.

청구항 28.
제27항에 있어서, 상기 복호화(905)를 하기 전에 하드디스크에 저장할 것인지의 여부를 판단하는 단계와;
하드디스크에 저장할 것이라고 선택되지 않은 경우에는 그대로 복호화(905)하고, 하드디스크에 저장할 것이라고 선택된 경우에는 하드디스크에 암호화된 콘텐트를 저장한 후에 복호화(905)를 행하도록 하는 단계;
를 더욱 구비하여 구성됨을 특징으로 하는 멀티미디어 스트리밍 콘텐트의 정보보호 방법.

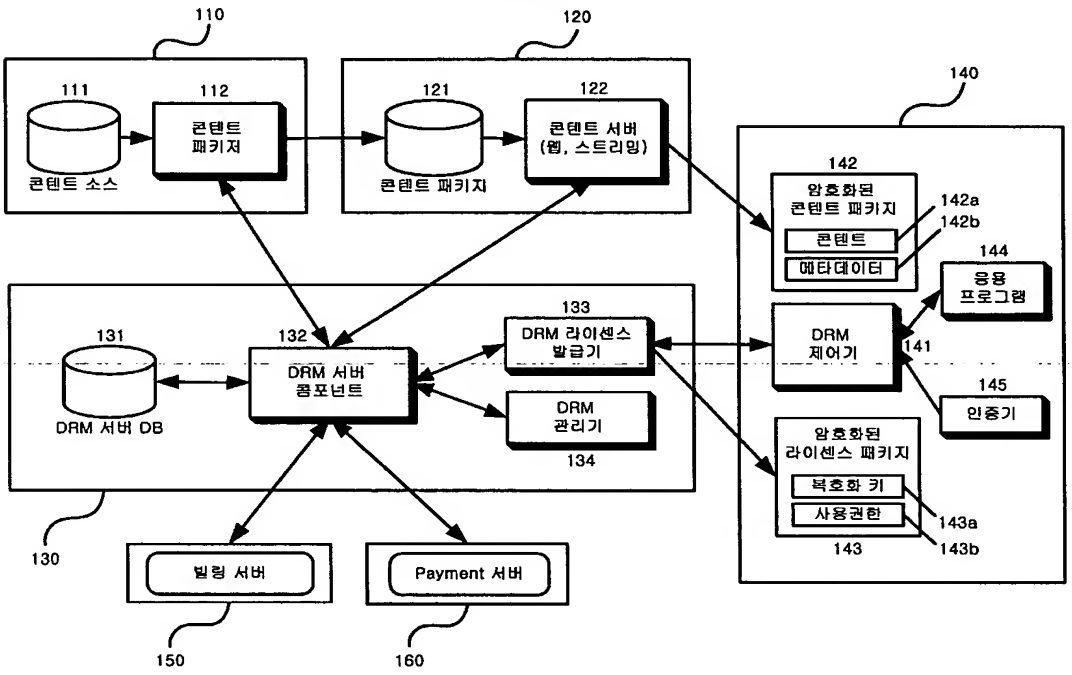
청구항 29.
제21항 또는 제23항에 있어서, 종료 및 연결해제 단계는
콘텐트 데이터를 복호화하고 플레이하는 매 주기마다 DRM 제어기(141)가 응용프로그램(144)의 종료 메시지를 검출하는 단계와;
종료 메시지가 검출되지 않으면 다시 복호화 및 플레이 단계로 진행하고, 종료 메시지가 검출되면 응용프로그램(144)을 종료시키고, 어드레스 핸들을 삭제함으로써 스트리밍 서버(122a)와의 연결을 해제시키는 단계;
로 구성됨을 특징으로 하는 멀티미디어 스트리밍 콘텐트의 정보보호 방법.

청구항 30.
각각 CPU, 휘발성 저장장치(메모리), 비휘발성 저장장치(하드디스크), 입출력장치(키보드, 모니터 등)를 가지며, 유무선 내부 통신수단이나 외부 네트워크와의 통신수단에 의하여 연결되어 있는 정보제공 시스템과 클라이언트 시스템을 이용하여 스트리밍되는 라이브/VOD 스트리밍 방식의 멀티미디어 콘텐트의 정보를 보호하는 방법이 저장된 컴퓨터로 실행할 수 있는 기록매체에 있어서,
콘텐트 소스(111)를 암호화하여 암호화된 콘텐트 패키지(121)로 만들어 콘텐트 서버(122)에 업로드하는 암호화 및 업로드 단계와;

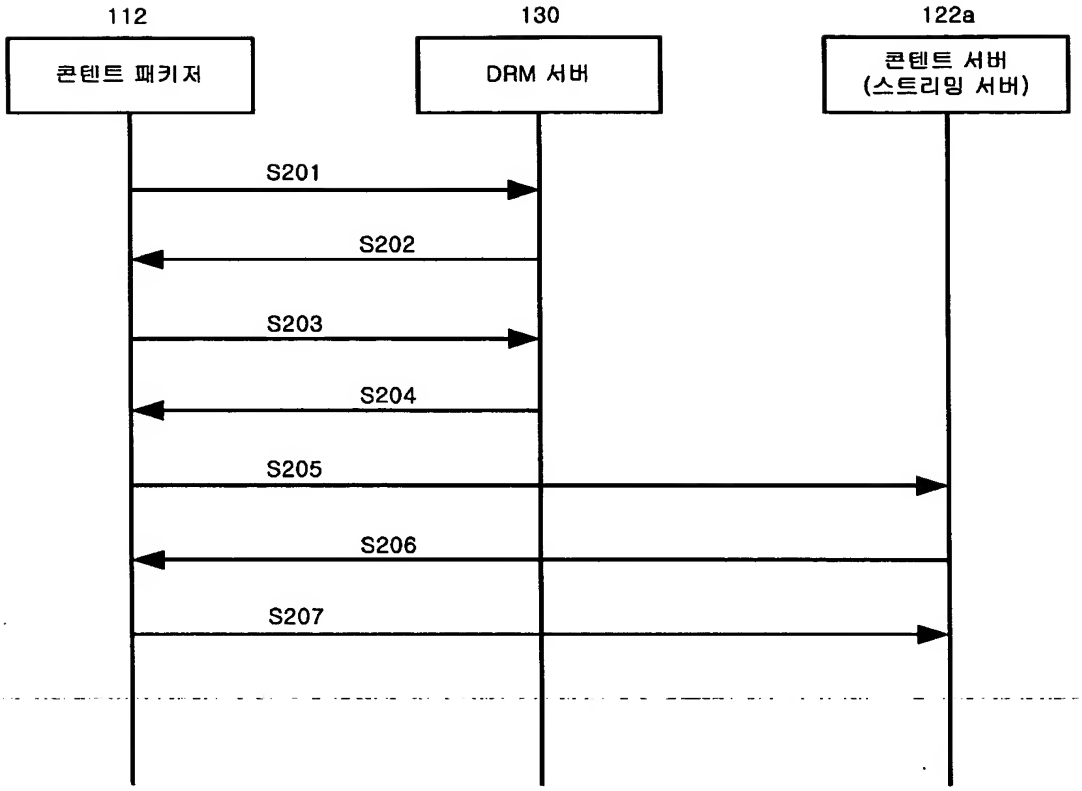
사용자가 웹 서버(122b) 또는 FTP 서버에서 선택함에 의하여 스트리밍 서버(122a)에 클라이언트 시스템을 연결하는 시작 및 연결 단계;
스트리밍되는 콘텐트 데이터를 복호화하면서 응용프로그램(144)을 통하여 플레이하는 복호화 및 플레이 단계;
응용프로그램(144)의 종료 메시지를 감지하여 종료하면서 스트리밍 서버(122a)와의 연결을 해제하는 종료 및 연결 해제 단계;
로 구성됨을 특징으로 하는 멀티미디어 스트리밍 콘텐트의 정보보호 방법이 저장되어 있는 컴퓨터로 실행할 수 있는 기록매체.

도면

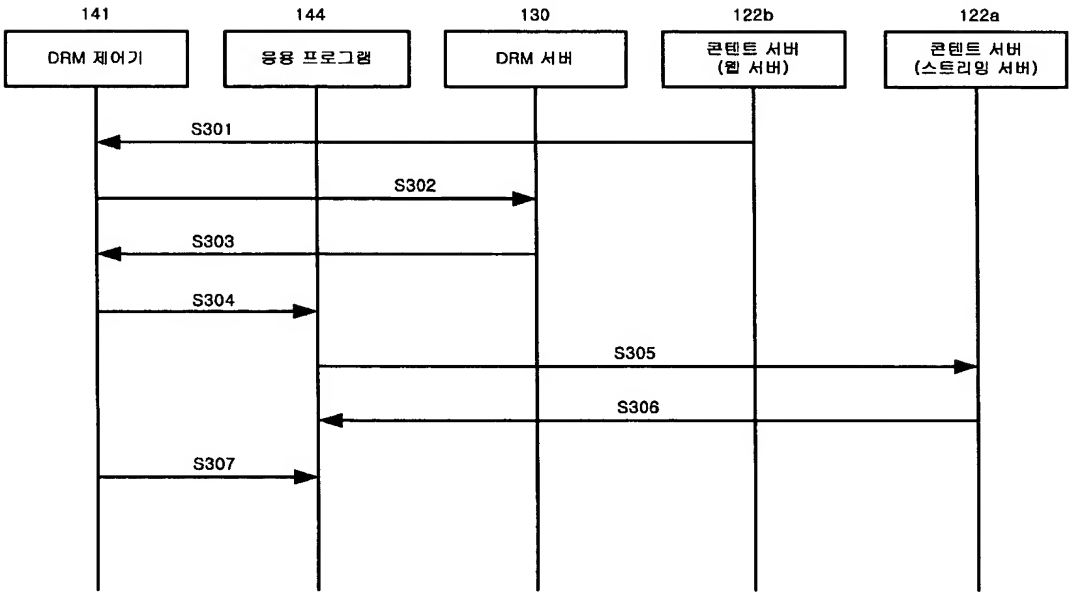
도면1



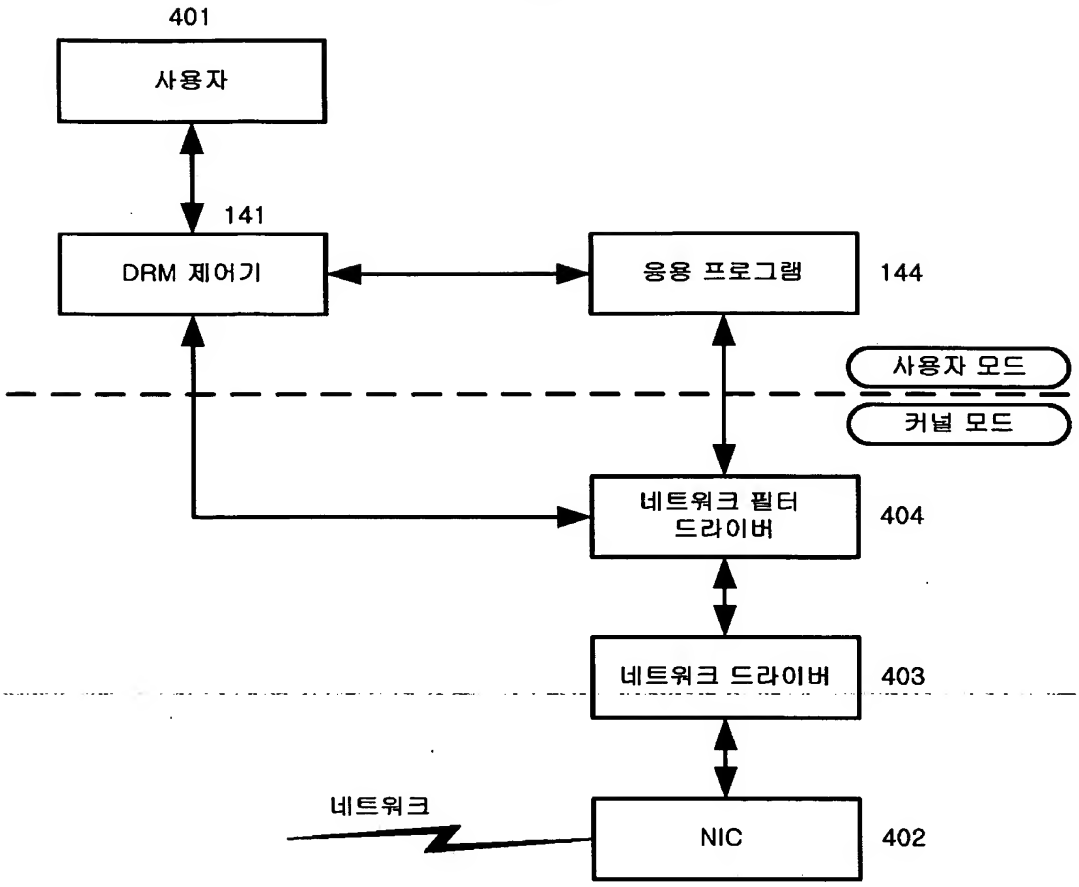
도면2


112
콘텐트 패키저
130
DRM 서버
122a
콘텐트 서버
(스트리밍 서버)
S201
S202
S203
S204
S205
S206
S207

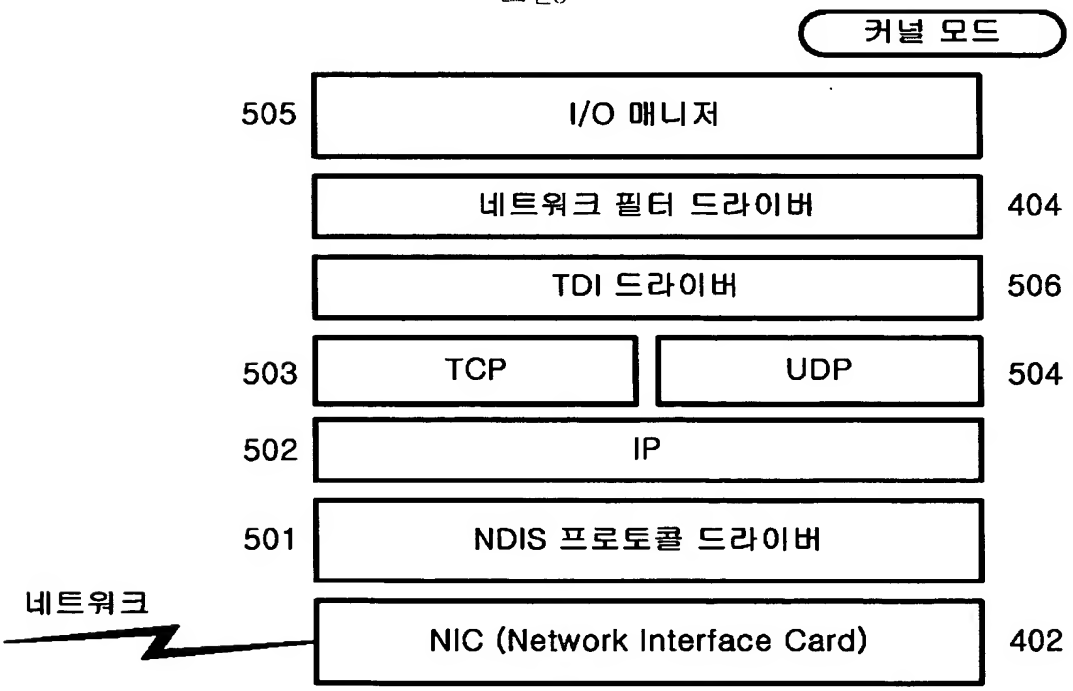
도면3


141
DRM 제어기
144
응용 프로그램
130
DRM 서버
122b
콘텐트 서버
(웹 서버)
122a
콘텐트 서버
(스트리밍 서버)
S301
S302
S303
S304
S305
S306
S307

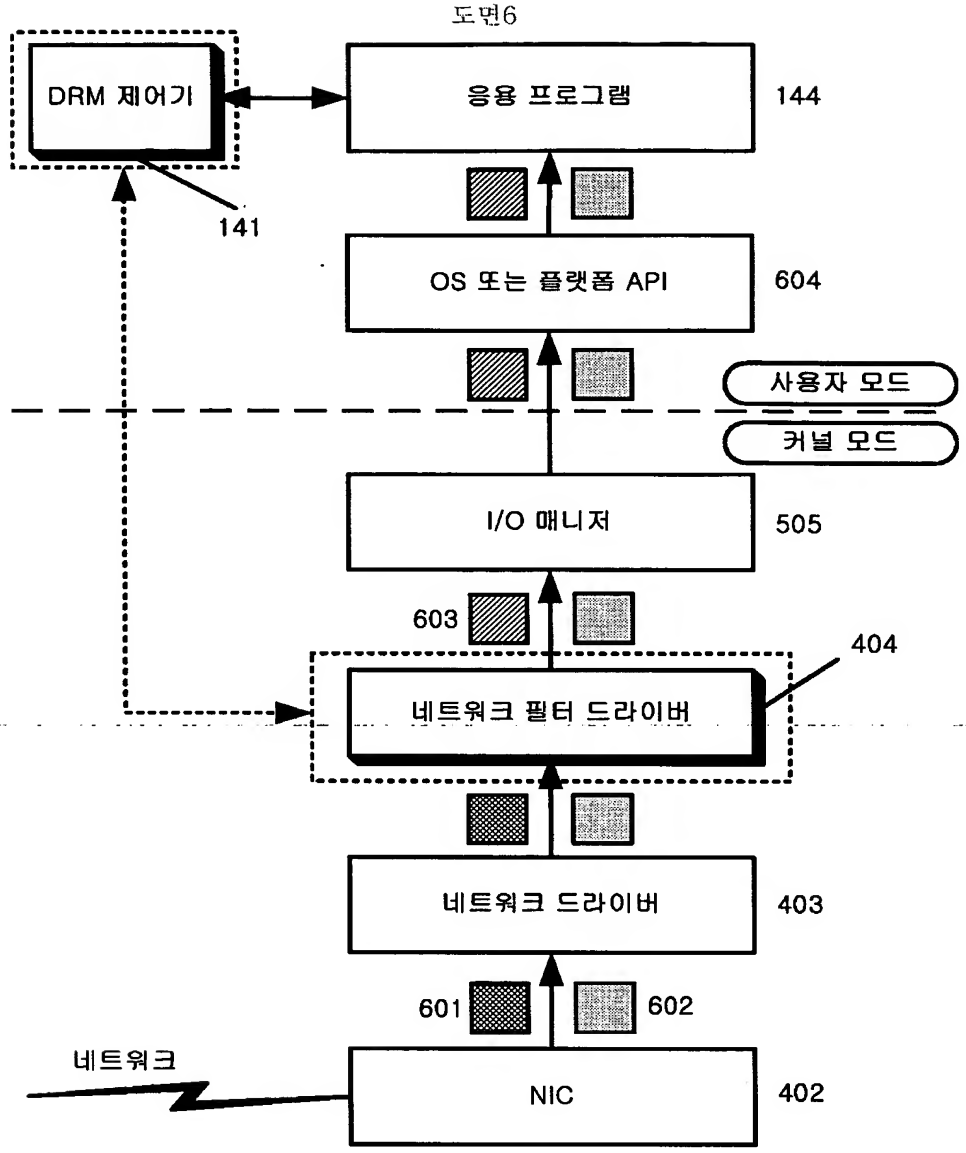
도면4


401
사용자
141
DRM 제어기
응용 프로그램
144
사용자 모드
커널 모드
네트워크 필터 드라이버
404
네트워크 드라이버
403
네트워크
NIC
402

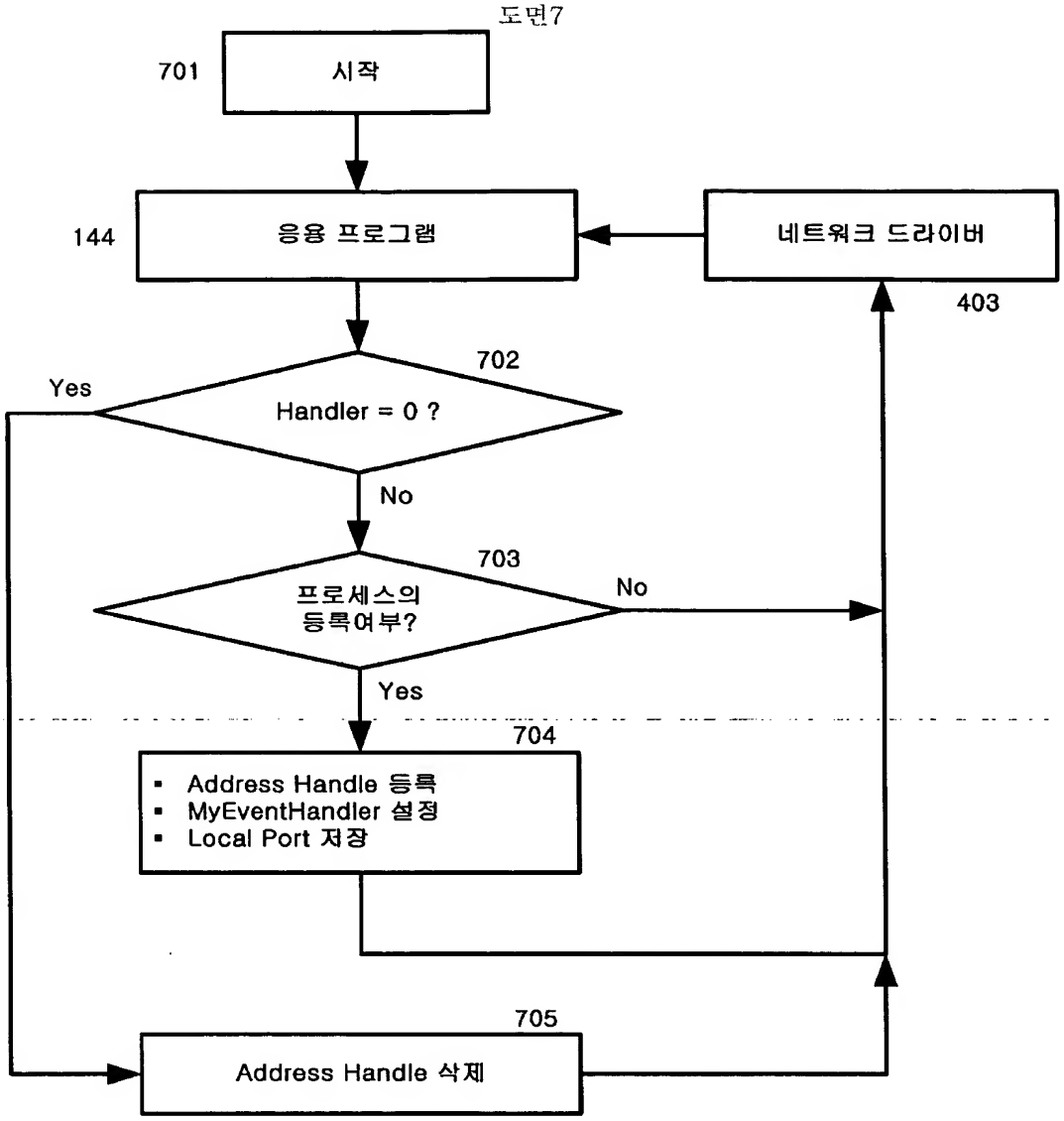
도면5


커널 모드
505
I/O 매니저
네트워크 필터 드라이버
404
TDI 드라이버
506
503
TCP
UDP
504
502
IP
501
NDIS 프로토콜 드라이버
네트워크
NIC (Network Interface Card)
402

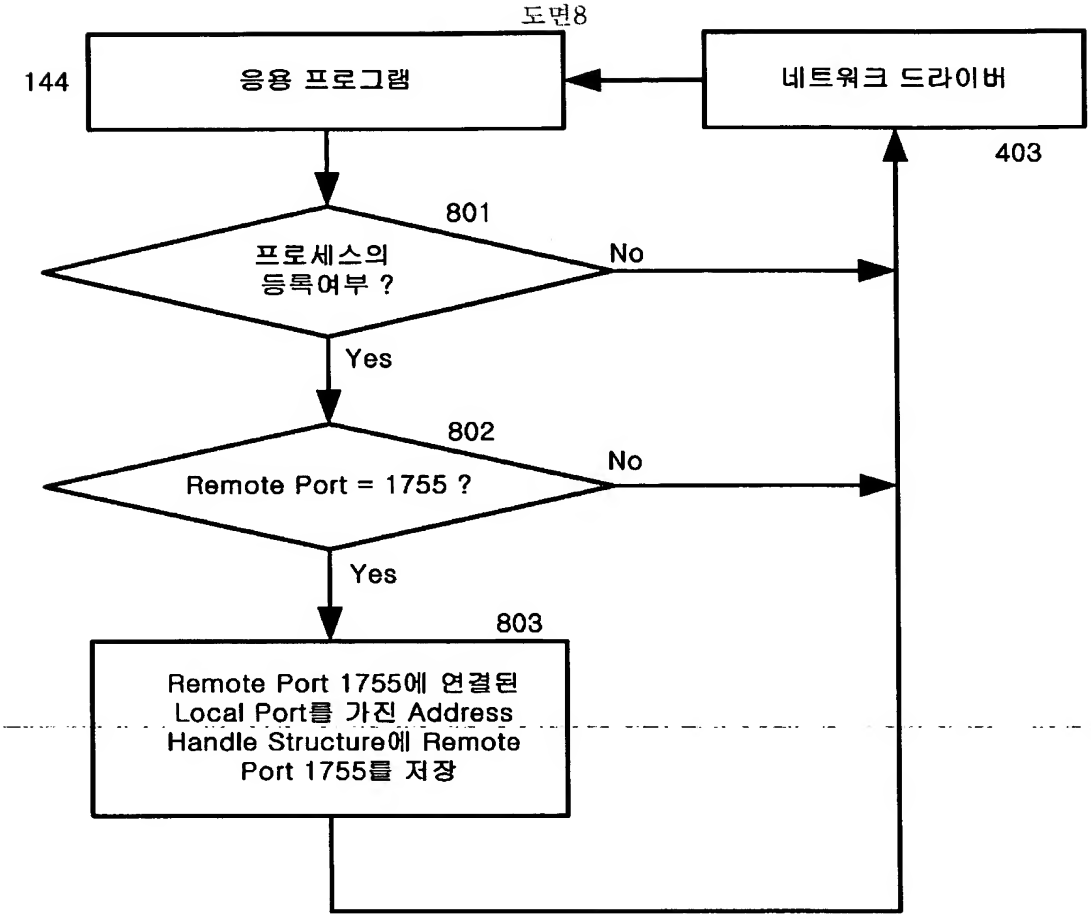
도면6


DRM 제어기
141
응용 프로그램
144
OS 또는 플랫폼 API
604
사용자 모드
커널 모드
I/O 매니저
505
603
404
네트워크 필터 드라이버
네트워크 드라이버
403
601
602
네트워크
NIC
402

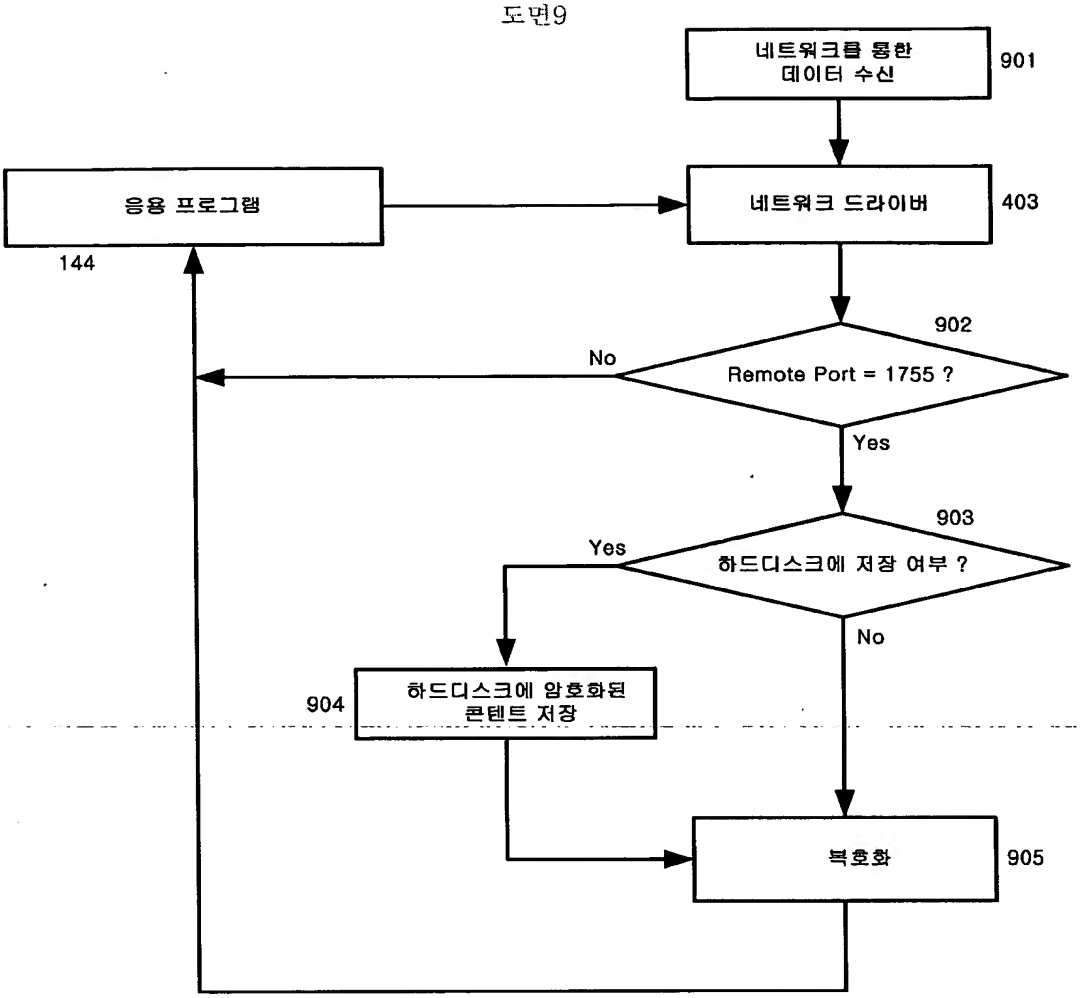
도면7


701
시작
144
응용 프로그램
네트워크 드라이버
403
702
Handler = 0 ?
Yes
No
703
프로세스의
등록여부?
No
Yes
704
Address Handle 등록
MyEventHandler 설정
Local Port 저장
705
Address Handle 삭제

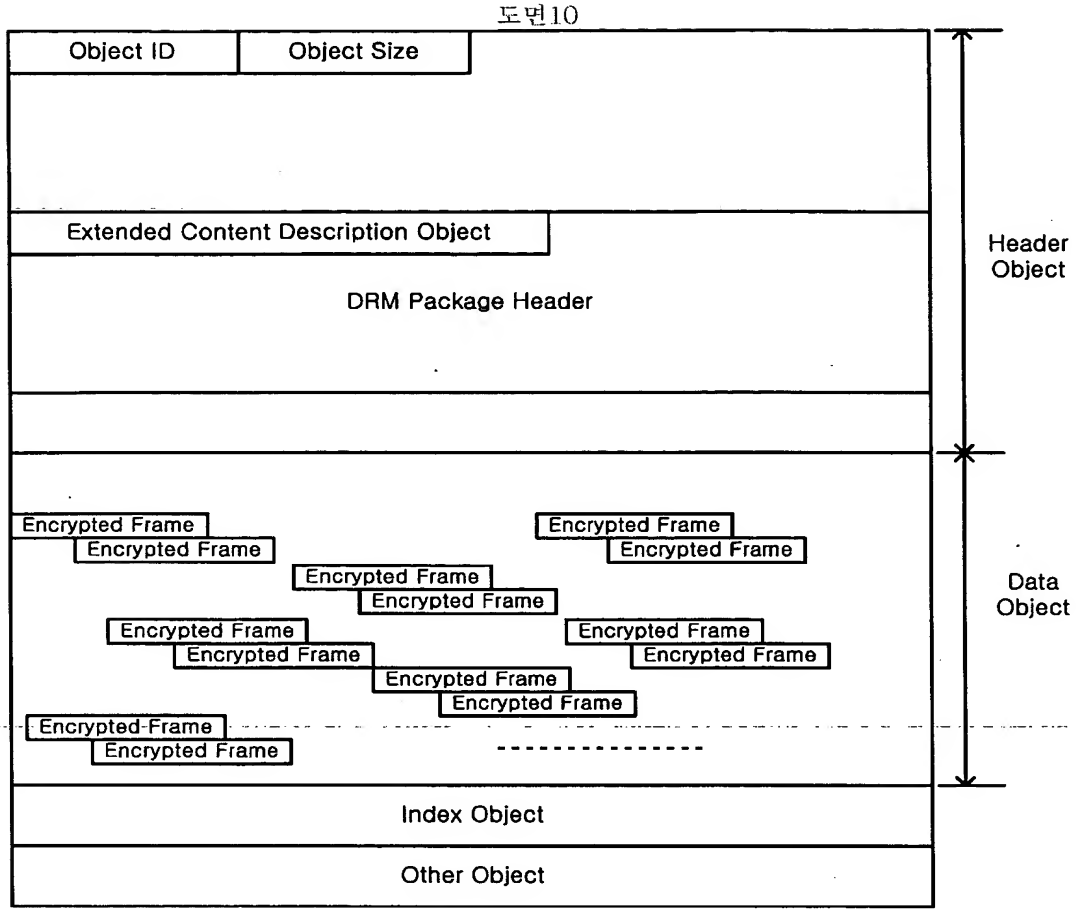
도면8


144
응용 프로그램
네트워크 드라이버
403
801
프로세스의
등록여부 ?
No
Yes
802
Remote Port = 1755 ?
No
Yes
803
Remote Port 1755에 연결된
Local Port를 가진 Address
Handle Structure에 Remote
Port 1755를 저장

도면9


네트워크를 통한
데이터 수신
901
응용 프로그램
144
네트워크 드라이버
403
902
Remote Port = 1755 ?
No
Yes
903
하드디스크에 저장 여부 ?
Yes
No
904
하드디스크에 암호화된
콘텐트 저장
복호화
905

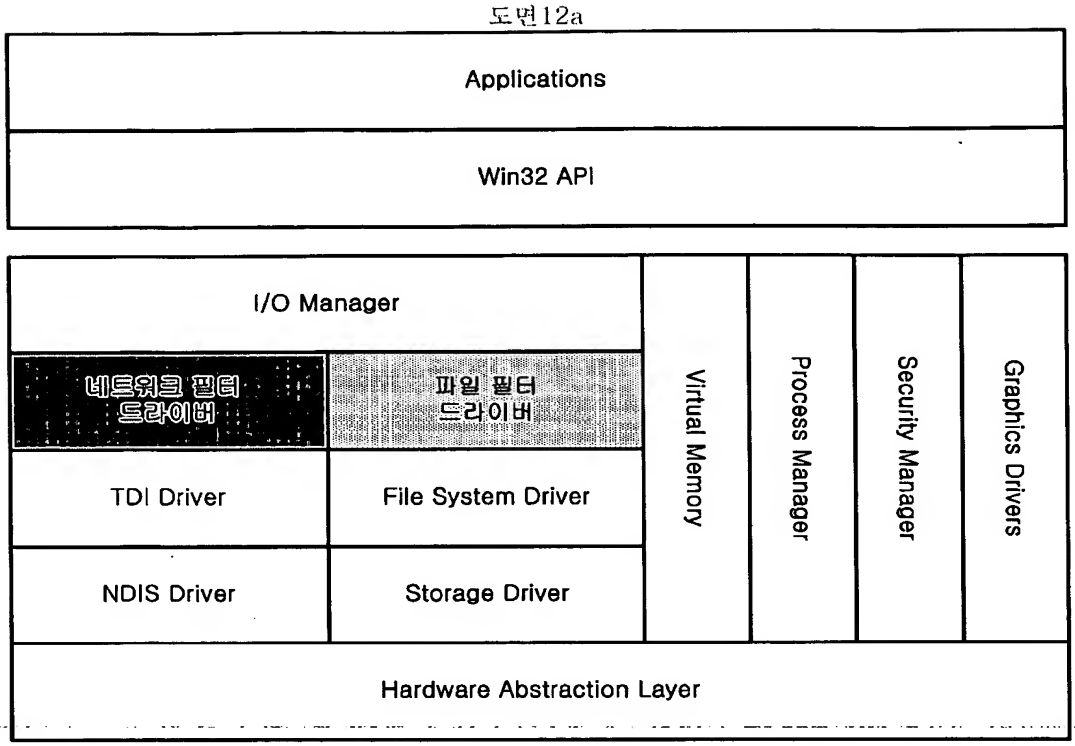
도면10



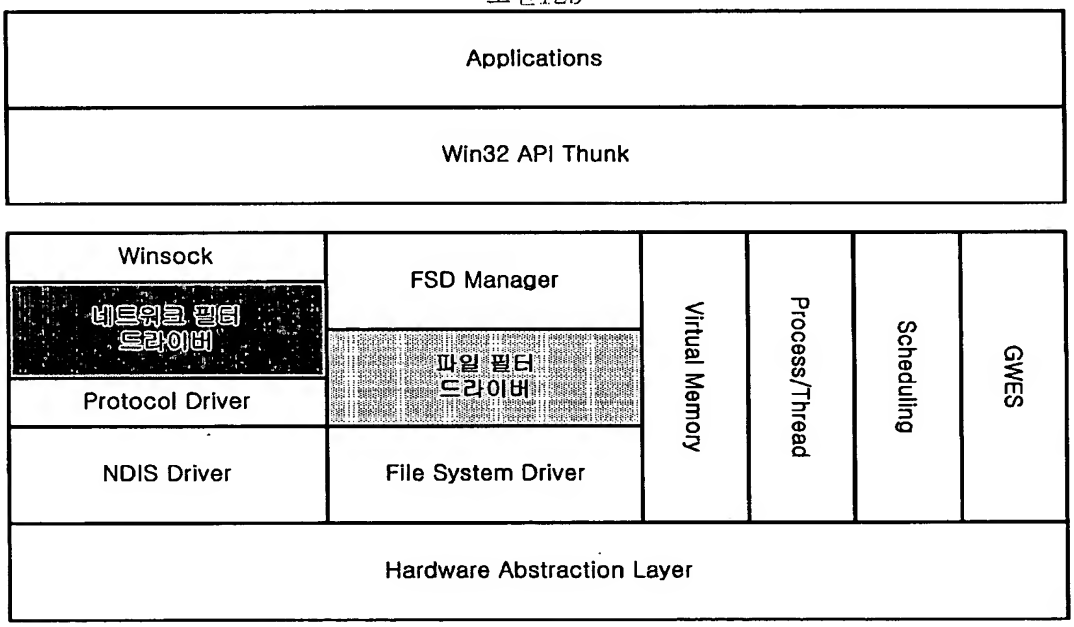
도면11

Version number	Content URI length	Content type length
Content URI		
Content type		
Header length	Data length	
Encryption Method		
Rights Issuer URL		
Content Name		
Content Description		
Content Vendor		
Icon URI		
Digital Signature	Content Server URL	

도면12a


Applications
Win32 API
I/O Manager
네트워크 필터 드라이버
파일 필터 드라이버
TDI Driver
File System Driver
NDIS Driver
Storage Driver
Virtual Memory
Process Manager
Security Manager
Graphics Drivers
Hardware Abstraction Layer

도면12b


Applications
Win32 API Thunk
Winsock
네트워크 필터 드라이버
Protocol Driver
FSD Manager
파일 필터 드라이버
NDIS Driver
File System Driver
Virtual Memory
Process/Thread
Scheduling
GWES
Hardware Abstraction Layer

GENERAL POWER OF ATTORNEY

Insert, in full, (a) the name and (b) address of the applicant

I/we, the undersigned, (a)
of (b)

do hereby appoint **KOREANA PATENT FIRM**, whose address is Dong-Kyong Bldg. 824-19, Yoksam-dong, Kangnam-ku, Seoul 135-080, Korea, as my/our lawful attorney(s), to take on my/our behalf proceedings for the followings:

all procedures relating to application for patent, utility model registration, design registration or trademark registration; all procedures relating to registration of patent, utility model, design or trademark right; abandonment of application for patent, utility model registration, design registration or trademark registration; withdrawal of application for patent, utility model registration, design registration or trademark registration; withdrawal of request relating to application for patent, utility model registration, design registration or trademark registration; withdrawal of petition relating to application for patent, utility model registration, design registration or trademark registration; withdrawal of application for registration of patent term extension; abandonment of patent, utility model, design or trademark right; claim of priority right based on patent application or utility model registration application under Article 55 (1) of the Patent Law or Article 18 of the Utility Model Law; withdrawal of claim of priority right based on patent application or utility model registration application under Article 55 (1) of the Patent Law or Article 19 of the Utility Model Law; appointment of sub-agents relating to application for patent, utility model registration, design registration or trademark registration; all procedures relating to request for trial against examiner뭘 decision of rejection with respect to application for patent, design registration or trademark registration; all procedures relating to request for trial against ruling to reject amendment with respect to application for design registration or trademark registration; all procedures relating to request for trial against ruling for revocation of patent, utility model registration or design registration; withdrawal of request for trial against examiner뭘 decision of rejection relating to application for patent, design registration or trademark registration; withdrawal of request for trial against ruling to reject amendment relating to application for design registration or trademark registration; withdrawal of request for trial against ruling for revocation of patent, utility model registration or design registration; request for examination on another person뭘 application for patent; all procedures relating to request for technical evaluation on a device with respect to (another person뭘) application for utility model registration or registered utility model; information furnishing on another person뭘 utility model registration or application for patent, design registration or trademark registration under Article 64 (2) of the Patent Law, Article 35 (6) of the Utility Model Law, Article 23-5 of the Design Law or Article 22 (3) of the Trademark Law; petition for preferential examination on another person뭘 application for patent or design registration under Article 61 of the Patent Law or Article 30 of the Design Law; Dual application to patent application based on utility model registration and utility model registration based on patent application; all procedures relating to request for trial against examiner뭘 decision of rejection of application for utility model registration; procedures relating to filing an opposition to patent, utility model registration, design registration or application for trademark registration; withdrawal of opposition to patent, utility model registration, design registration or application for trademark registration; all procedures relating to trial of patent, utility model registration, design registration or trademark registration; withdrawal of demand for trial of patent, utility model registration, design registration or trademark registration; withdrawal of request relating to trial of patent, utility model registration, design registration or trademark registration; appointment of sub-agents relating to trial of patent, utility model registration, design registration or trademark registration; all procedures relating to application for registration for conversion of classification of goods; all procedures relating to registration for conversion of classification of goods; withdrawal of application for registration for conversion of classification of goods; all procedures relating to request for trial against examiner뭘 decision of rejection with respect to application for registration for conversion of classification of goods; all procedures relating to request for trial against ruling to reject amendment with respect to application for registration for conversion of classification of goods; withdrawal of request for trial against examiner뭘 decision of rejection relating to application for registration for conversion of classification of goods; and withdrawal of request for trial against ruling to reject amendment relating to application for registration for conversion of classification of goods. (A01 □D26)

Dated this day of , 20

(c) Corporation name in full in the case of a corporation; otherwise to be left blank.

(c) _____

(d) Signature of the per-son appointing the attor-ney(s). In the case of a corporation, the signature should be that of the Pre-sident, Director or other authorized representative.

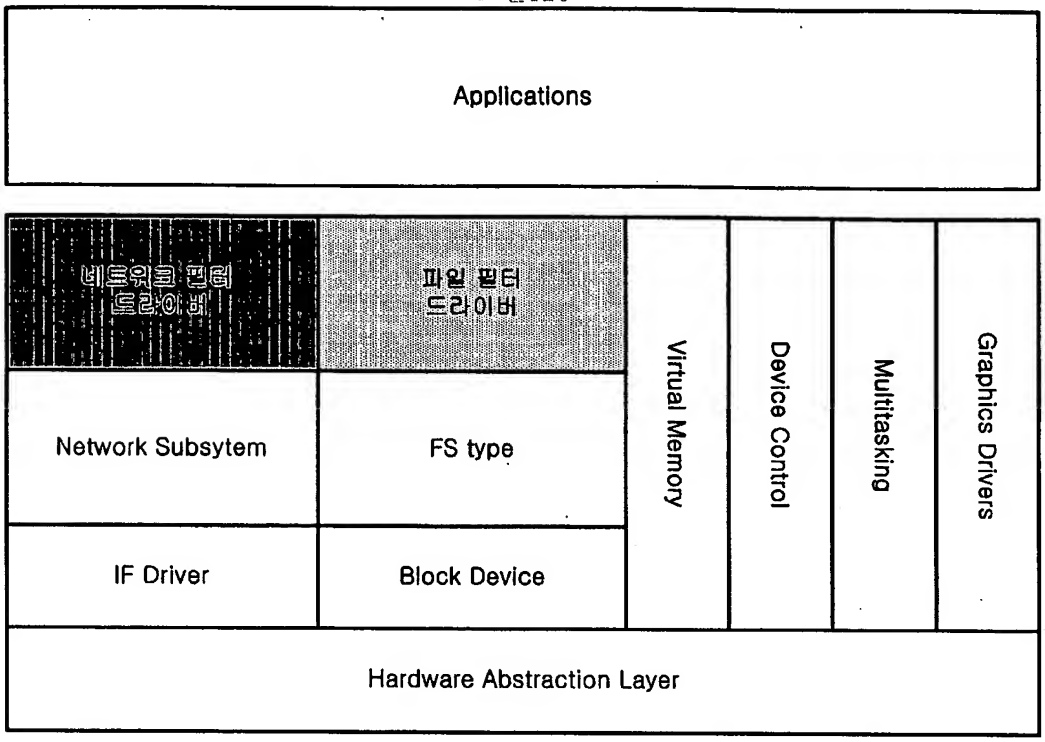
By (d) _____
(e)

MOST IMPORTANT

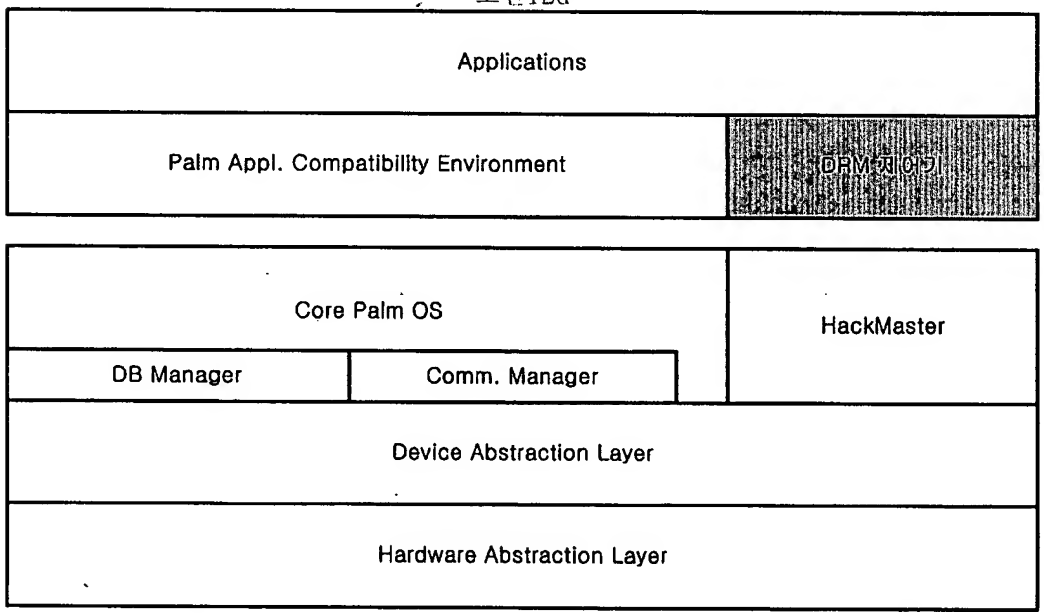
(e) TYPE FULL NAME OF SIGNATORY

(NO NOTARIZATION)

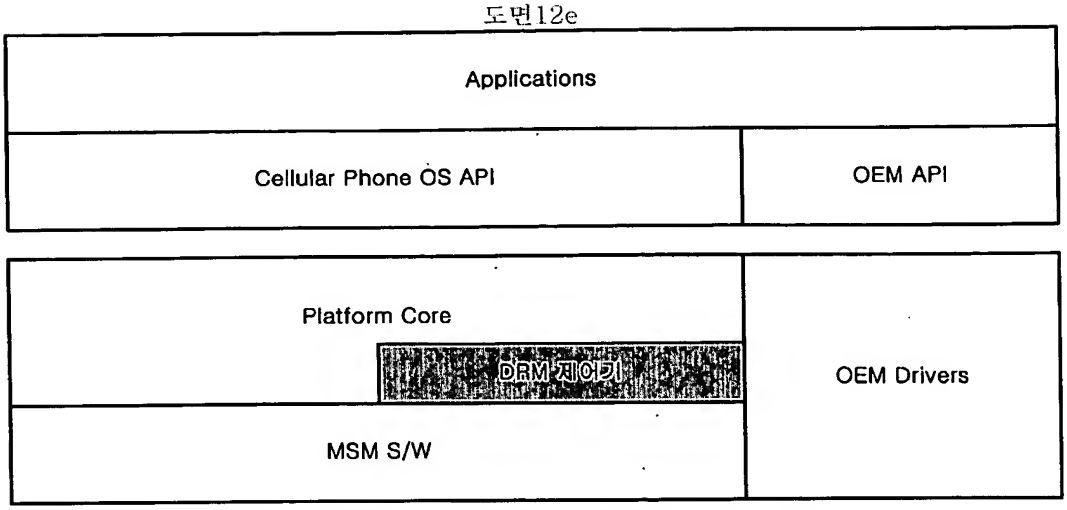
도면12c


Applications
네트워크 관련 드라이버
파일 필터 드라이버
Virtual Memory
Device Control
Multitasking
Graphics Drivers
Network Subsytem
FS type
IF Driver
Block Device
Hardware Abstraction Layer

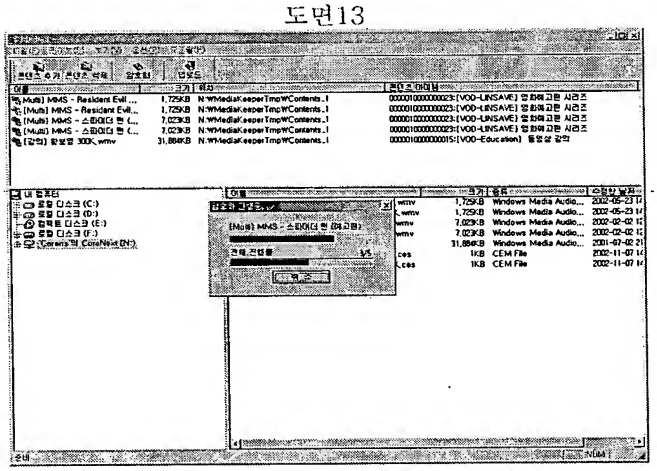
도면12d


Applications
Palm Appl. Compatibility Environment
DRM 제어기
Core Palm OS
HackMaster
DB Manager
Comm. Manager
Device Abstraction Layer
Hardware Abstraction Layer

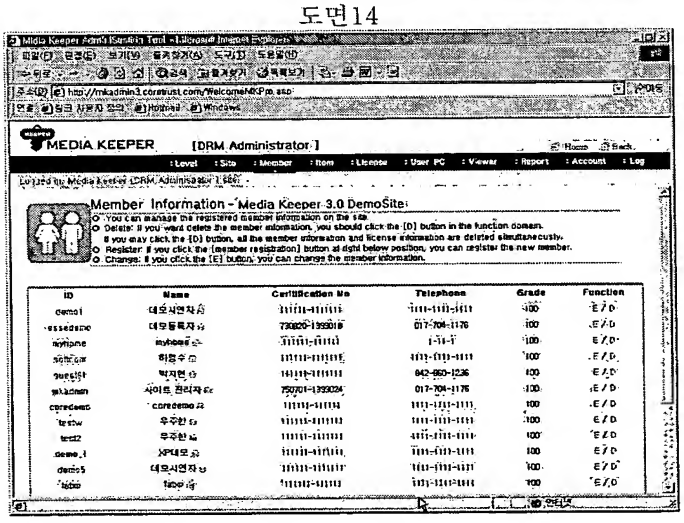
도면12e



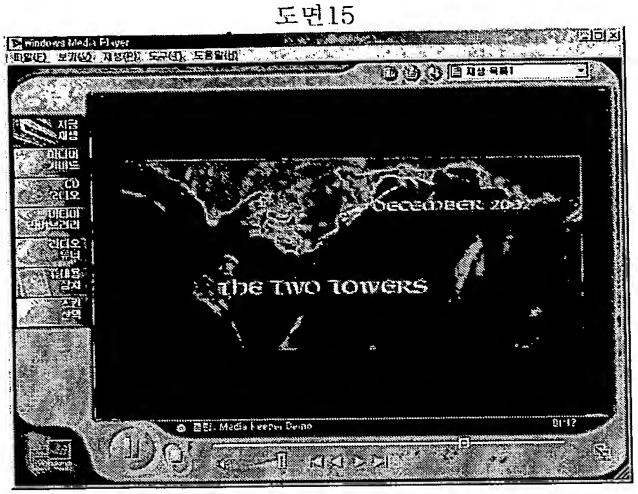
도면13



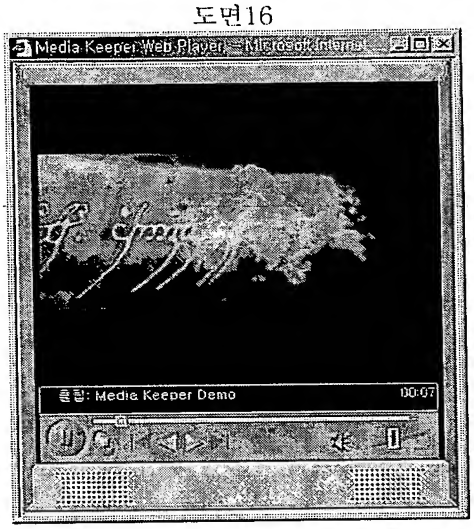
도면14



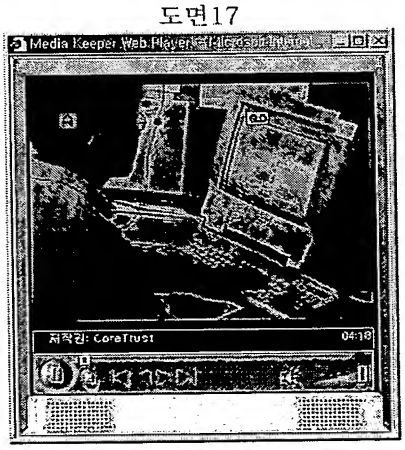
도면15



도면16



도면17



도면18

(19) KOREAN INTELLECTUAL PROPERTY OFFICE

KOREAN PATENT ABSTRACTS

(11)Publication number: 1020020075568 A
(43)Date of publication of application: 05.10.2002

(21)Application number: 1020010015639
(22)Date of filing: 26.03.2001

(71)Applicant: SAMSUNG ELECTRONICS CO., LTD.
(72)Inventor: KIM, BYEONG JUN
KO, JEONG WAN

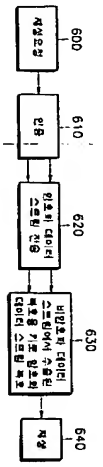
(51)Int. Cl G11B 20/10

(54) CODED DATA INCLUDING DATA TRANSMITTING AND RECEIVING CONTROL METHOD

(57) Abstract:

PURPOSE: A method for controlling the transmitting and receiving of data including coded data is provided to safely transmit pay data to various business models by employing coding method of selective data streams, thereby preventing any additional copy of the reproduced coded data without permission.

CONSTITUTION: A method for controlling the transmitting and receiving of data including coded data includes the steps of transmitting channel data, in which image information is coded, together with non-coded channel data in the multiple streaming mode(620), wherein key required for decoding the stream data of the coded channel is inserted into stream data of the non-coded channel in the vicinity(630).



Legal Status
Date of final disposal of an application (20031128)
Patent registration number (1004136820000)
Date of registration (20031219)

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl. [7]
G11B 20/10

(11) 공개번호 특2002-0075568
(43) 공개일자 2002년10월05일

(21) 출원번호 10-2001-0015639
(22) 출원일자 2001년03월26일

(71) 출원인 삼성전자 주식회사
경기 수원시 팔달구 매탄3동 416

(72) 발명자 김병준
경기도수원시팔달구우만2동29번지주공아파트207동404호
고정완
경기도용인시이동면서리684-6

(74) 대리인 이영필
이해영

심사청구 : 있음

(54) 암호화된 데이터를 포함한 데이터의 전송 및 수신 제어 방법

요약

본 발명은 암호화 데이터의 전송 및 수신 제어 방법에 관한 것으로서, 암호화가 필요한 채널의 전송 및 수신 제어 방법은, 암호화할 채널의 데이터 중 일부만을 암호화하여 소정의 스트리밍 방식으로 전송하고, 상기 암호화된 스트림을 복호화하기 위한 키를 암호화되지 않은 이웃 스트림에 삽입하여 전송하는 단계; 상기 이웃 스트림으로부터 상기 복호용키를 추출하는 단계; 및 상기 복호용 키를 사용하여 상기 암호화된 데이터 스트림을 복호화하여 재생하는 단계를 포함함을 특징으로 한다.

본 발명에 의하면 선택적 데이터 스트림의 암호화 방식을 채용함으로써 다양한 비즈니스 모델에 유료 데이터를 안전하게 전송할 수 있고 억세스 되어 재생된 암호화 데이터에 대해 추가 복제를 방지할 수 있다.

대표도
도 6

명세서

도면의 간단한 설명

도 1a ~ 도 1b는 일반적인 디지털 방식의 다중 스트림 데이터 전송 또는 기록 포맷을 보인 것이다.

도 2a ~ 도 2b는 도 1a ~ 도 1b와 같은 다중 스트림의 기록 또는 전송 포맷에 있어서, 선택적인 채널만이 암호화되어 전송 또는 기록됨을 보이는 본 발명에 따른 데이터 전송 포맷의 예이다.

도 3은 본 발명의 다중 스트림의 선택적 암호화 전송 방법의 흐름을 보인 블록도이다.

도 4는 본 발명의 암호화 데이터 스트림의 다른 전송 포맷을 보인다.

도 5는 본 발명의 다중 데이터 스트림의 선택적 암호화 전송 포맷의 예를 보인다.

도 6은 도 5와 같은 암호화 데이터 스트림 전송 및 재생 동작의 흐름도를 도시한 것이다.

도 7은 도 6과 같은 전송 제어가 이뤄질 때 수신측에서의 암호화 스트림 억세스 제어 과정을 보다 상세히 도시한 흐름도이다.

도 8은 한번 녹화하면 재생할 수는 있지만 다시 복사 할 수는 없는 일회 기록 방식 미디어의 기록 및 재생 제어방식의 흐름도이다.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 데이터 전송 및 수신 제어 방법에 관한 것으로서, 보다 상세하게는 전송할 데이터 스트림의 종류나 비즈니스 모델에 따라 데이터 스트림을 선택적으로 암호화하여 전송하고 억세스하는 암호화된 데이터를 포함한 데이터의 전송 및 수신 제어 방법에 관한 것이다.

디지털 방송이 시작되고 디지털 미디어가 보급되면서 다양한 복제 방지 기술과 장치들이 개발되고 왔다. 그러한 기술과 장치는 대부분 단일 스트리밍 방식에 적용되거나 스트림의 종류에 상관없이 적용되는 경우가 일반적이다.

예를 들어, 복제를 방지하기 위해 데이터를 암호화하는 기술은 디브이디(DVD) 에서 흔하게 적용되고 있는데, 이것은 데이터 전체 또는 일부를 암호화하여 기록한 후 재생시에는 그 데이터를 복호한 후 화면에 표시하기만 하며 데이터를 직접 복제 할 수는 없도록 되어 있다. 이러한 암호화 기술을 다른 기록 가능 미디어에 적용할 수도 있다. 암호화된 데이터가 기록된 미디어에 접근하기 위해서, 해당 미디어에 접근 권한이 있는 스마트 카드나 비밀번호 입력 방식 또는 중앙 시스템에서 해당 미디어 재생 장치를 직접 제어하는 방식과 같은 접근 제어 방식이 있다. 디지털 방송의 경우 암호화가 채용되는 유료방송에 대한 규격이 존재하는데 이것은 단일 스트리밍 방식이므로 보다 다양한 비즈니스 모델에서는 그런 규격의 이용이 제약을 받게된다.

이러한 암호화 전송 방식은 부가적인 비즈니스 모델에 적용하거나 한번 복호화한 후 저장되는 시점에서 데이터 보호가 되지 않는 문제가 발생할 수도 있다. 또 항상 동일한 키 정보를 이용해서 해당 데이터 스트림을 복호하므로 안전성에 문제가 생길 수 있다.

발명이 이루고자 하는 기술적 과제

본 발명이 이루고자 하는 기술적 과제는, 전송할 데이터 스트림의 종류나 비즈니스 모델에 따라 데이터 스트림을 선택적으로 암호화하여 전송하고 억세스하는 암호화된 데이터를 포함한 데이터의 전송 및 수신 제어 방법을 제공하는데 있다.

발명의 구성 및 작용

상기 과제를 해결하기 위한, 영상 정보 전송 방법은, 비암호화 채널 데이터와 함께, 상기 영상 정보를 암호화한 채널 데이터를 다중 스트리밍 방식으로 전송하는 단계를 포함하고, 이때 상기 암호화된 채널의 스트림 데이터를 복호화하는데 필요한 키를 인접하는 비암호화된 채널의 스트림 데이터에 삽입하여 전송함을 특징으로 한다.

상기 암호화 채널의 데이터 중 일부 스트림 데이터만이 암호화되어 전송됨이 바람직하다.

상기 암호화 채널의 전체 스트림 데이터는 모두 암호화되어 전송됨이 바람직하다.

상기 과제를 해결하기 위한, 암호화가 필요한 채널의 데이터를 전송하는 방법은, 암호화할 채널의 데이터 중 일부만을 암호화하여 소정의 스트리밍 방식으로 전송하는 단계를 포함하고, 이때 상기 암호화된 데이터를 복호화하기 위한 키를 상기 동일 채널의 스트림 데이터 중 암호화되지 않은 스트림내에 삽입하여 전송함을 특징으로 한다.

상기 과제를 해결하기 위한, 암호화가 필요한 채널의 전송 및 수신 방법은, 암호화할 채널의 데이터 중 일부만을 암호화하여 소정의 스트리밍 방식으로 전송하고, 상기 암호화된 스트림을 복호화하기 위한 키를 암호화되지 않은 이웃 스트림에 삽입하여 전송하는 단계; 상기 이웃 스트림으로부터 상기 복호용키를 추출하는 단계; 및 상기 복호용 키를 사용하여 상기 암호화된 데이터 스트림을 복호화하여 재생하는 단계를 포함함을 특징으로 한다.

상기 과제를 해결하기 위한, 소정 전송 스트리밍 방식으로 전송된 암호화 데이터 스트림과 비암호화 데이터 스트림을 저장 매체에 기록(녹화)하여 재생하는 방법은, 전송된 데이터 스트림으로부터 암호화 스트림을 복호화하기 위한 키를 추출하여 상기 저장 매체의 소정 영역에 저장하는 단계; 전송된 암호화 스트림과 비암호화 스트림을 저장 미디어의 데이터 영역에 저장하는 단계; 및 상기 복호용 키를 이용하여 상기 암호화 스트림을 복호화하는 단계를 포함함을 특징으로 한다.

상기 복호용 키가 저장되는 상기 저장매체의 소정 영역은, 상기 암호화된 데이터 스트림이 외부로 복제되어 재생될 수 없도록 사용자 접근 및 저장 데이터이 외부로의 복제가 불가능한 영역임이 바람직하다.

상기 과제를 해결하기 위한, 광고 콘텐츠와 사용자 이용 콘텐츠를 전송 및 수신하는 방법은, 상기 광고 콘텐츠는 암호화하지 않고 상기 사용자 이용 콘텐츠는 암호화하는 단계; 상기 광고 콘텐츠에 해당하는 스트림에 상기 암호화된 사용자 이용 콘텐츠를 복호화하는데 필요한 키를 삽입하는 단계; 상기 복호용 키가 삽입된 광고 콘텐츠를 상기 암호화된 사용자 이용 콘텐츠 앞에 위치시켜 전송하는 단계; 상기 광고 콘텐츠를 수신하여 시청하면 상기 복호용 키가 추출되어지는 단계; 및 상기 복호용 키를 이용하여 상기 사용자 이용 콘텐츠의 암호 데이터를 복호화하는 단계를 포함함을 특징으로 한다.

상기 광고 콘텐츠를 사용자가 일정 시간 시청하도록, 상기 복호용 키는 상기 광고 콘텐츠의 소정 부분에 분산되어 들어 있음이 바람직하다.

이하에서 첨부된 도면을 참조하여 본 발명을 상세히 설명한다.

도 1a ~ 도 1b는 일반적인 디지털 방식의 다중 스트림 데이터 전송 또는 기록 포맷을 보인 것이다. 도 1a는 시간분할을 이용한 디중 스트림의 전송 포맷의 예로서 세 개의 채널, 즉 채널 1, 채널 2, 채널 3이 각각 시분할되어 채널 1-0, 채널 2-0, 채널 3-0, 채널 1-1, 채널 2-1, 채널 3-1, 채널 1-2, 채널 2-2,..등의 스트림 데이터로 기록 또는 전송되는 포맷이다. 도 1b는 주파수분할을 이용한 다중 스트림 전송 포맷의 예로서 세 개의 채널이 주파수분할되어 기록 또는 전송되는 포맷이다.

도 2a ~ 도 2b는 도 1a ~ 도 1b와 같은 다중 스트림의 기록 또는 전송 포맷에 있어서, 선택적인 채널만이 암호화되어 전송 또는 기록됨을 보이는 본 발명에 따른 데이터 전송 포맷의 예로서, 여기서 암호화된 채널은 채널 2이다. 도 2a ~ 도 2b에서 암호화된 채널 2는 채널 2의 데이터 스트림 안에 암호화된 데이터의 복호화에 필요한 키 정보가 함께 삽입된 채 전송되거나 채널 2 스트림 전송 이전에 해독에 필요한 복호화 키 정보가 주어져야 한다.

도 3은 본 발명의 다중 스트림의 선택적 암호화 전송 방법의 흐름을 보인 블록도이다. 먼저 재생 또는 시청 요청이 들어오면(300단계), 요청한 주체에 대해 인증 과정을 수행한다(310단계). 인증이 이뤄지면 요청한 주체에 접근 권한을 부여하고, 복호용 키와 함께 암호화된 데이터 스트림을 전송한다(320단계). 인증 과정(310단계)은 방송국 등 전송을 담당하는 지점과 수신하는 단말기 사이에서 이뤄지고, 미디어의 경우 미디어를 읽는 부분과 재생을 담당한 부분 사이에서 이뤄진다. 복호용 키 전송 및 암호화된 데이터 스트림의 전송은 방송국과 미디어를 읽는 부분에서 수행한다. 복호용 키는 별도로 전송되거나 암호화된 데이터 스트림안에 숨겨져서 보내어질 수 있다. 단말기나 미디어 재생 부분은 전송된 복호화 키와 암호화된 데이터 스트림을 수신하여 확인하고 암호화된 데이터를 복호화하여(330단계) 재생(또는 시청)을 시작한다(340단계).

도 4는 본 발명의 암호화 데이터 스트림의 다른 전송 포맷을 보인다. 이 포맷은 전송 후 디멀티플렉싱된 한 채널만이 도시된 것이다. 여기에서, 종래와 달리 채널의 특정 부분(스트림 2-0, 2-6)에 복호화 키를 삽입하여 전송함을 알 수 있다. 수신측에서는 이 특정부분의 스트림을 수신하여 재생하거나 시청하지 않으면 나머지 스트림의 영역을 재생할 수 없도록 된다. 이 경우 스트림 2-0과 스트림 2-6에 서로 다른 복호화 키를 삽입함으로써, 하나의 복호화 키만으로는 전체 스트림을 해독하여 재생할 수 없고, 스트림 전송시 복호화 키를 수시로 바꿀 수 있어 보호하고자 하는 데이터 스트림을 안전하게 보호할 수 있다.

도 5는 본 발명의 다중 데이터 스트림의 선택적 암호화 전송 포맷의 예를 보인다. 이 전송 방식에서는 암호화하려고 하는 스트림(스트림 2)(500)에 대한 복호 키를 인접하는 다른 스트림(스트림 1 또는 스트림 3)(510 또는 520)에 포함시켜 전송한다. 이 경우 다양한 비즈니스 모델에 대한 암호화 전송을 구현할 수 있고, 암호화된 스트림을 해독할 키 정보를 별도로 전송하지 않으며, 암호화할 데이터를 보호하기 위해 전송 중에 임의로 키 정보를 변경가능하다. 또한 복호용 키를 인접한 스트림내에 숨겨서 보내기 때문에 기록할 당시의 상황(동시에 스트림 1, 2, 3가 방송되는 상황)에서가 아니면 복호용 키를 구할 수 없다. 따라서 스트림 2만을 녹화하여 재생하거나 복제하는 것이 불가능하다.

도 6은 도 5와 같은 암호화 데이터 스트림 전송 및 재생 동작의 흐름도를 도시한 것이다. 재생 요청(또는 시청 요청)이 있은 후(600단계) 전송측 또는 방송국에서는 재생 가능여부를 인증하는 인증 과정을 수행한다(610단계). 인증은 전송측과 수신측 쌍방간의 소정의 확인 절차에 따라 진행된다. 인증이 끝나면 전송측에서는 암호화된 데이터 스트림을 전송한다(620단계). 수신측은 암호화된 스트림이 전송되었는지를 확인하고 인접 스트림에 포함된, 암호 스트림을 복호화할 키를 사용하여 암호화된 스트림을 복호한 후(630단계) 재생을 시작한다(640단계).

도 7은 도 6과 같은 전송 제어가 이뤄질 때 수신측에서의 암호화 스트림 억세스 제어 과정을 보다 상세히 도시한 흐름도이다.

전송된 암호화 스트림을 확인하고(700단계), 암호화되지 않은 스트림이 재생되도록 한다(710단계). 재생중인 암호화되지 않은 스트림으로부터 암호화된 스트림을 복호화할 키를 추출한다(720단계). 추출한 복호화 키를 사용하여 암호화되지 않은 스트림을 복호화한다(730단계). 복호화한 스트림을 재생한다(740단계).

도 6 및 도 7과 같은 암호화 방법 및 암호화 데이터 접근 방법은, 비암호 스트림을 원하는 광고로, 암호 스트림은 사용자가 필요로 하는 방송 내용으로 채워, 광고 스트림을 일정시간 수신하여 재생하면 그로부터 복호화 키를 추출할 수 있고, 그 추출된 키를 이용해 광고 이후 전송되는 암호화된 스트림에 대해 복호화를 가능하게 하는 식의, 일정시간 동안 광고를 시청하면 암호화된 방송을 무료로 볼 수 있게하는 등의 방송 비즈니스에 이용될 수 있다. 사용자가 광고에 해당하는 비암호 스트림을 보는 도중 그 스트림안에 숨겨지거나 암호화되거나 워터마크등을 사용해 감춰진 복호용 키를 읽어내어 이후에 들어오는 소정 채널의 암호화된 스트림을 복호화할 수 있다. 광고 채널의 스트림을 전송하면서 수신자가 광고를 일정 시간 동안 보기를 원하면, 전송측에서는 암호화되지 않은 광고 채널 스트림상에 일정 간격을 둔 채 복호화 키를 삽입하고 이후에 들어오는 암호화된 채널 스트림을 전송하면, 수신자가 일정 시간 광고를 수신한 이후에야 인접한 암호화된 채널 스트림의 암호 해독을 위한 복호화 키를 얻을 수 있게된다. 이런 전송방식은 스포츠 유료 방송 공급자가 스포츠 중계 사이 사이에 광고를 삽입하고 수신자가 광고를 일정 시간 시청하면 이후에 중계되는 스포츠가 재생될 수 있도록 하는 등의 비즈니스 모델에 채용될 수 있다.

도 8은 한번 녹화하면 재생할 수는 있지만 다시 복사 할 수는 없는 일회 기록 방식 미디어의 기록 및 재생 제어방식의 흐름도이다. 수신된 데이터 스트림을 최초로 미디어에 녹화(기록)시에 먼저 암호화되지 않은 비암호 데이터 스트림으로부터 복호용 키를 읽어내고 이 키가 보관되었던 원래 영역을 의미없는 값으로 변경한다(800단계). 추출한 복호용 키를 미디어의 특정 영역에 저장해둔다(810단계). 상기 특정 영역은 사용자가 접근하거나 수정할 수 없는 영역이어야 한다. 비암호 스트림과 암호 스트림을 모두 미디어의 데이터 기록 영역에 기록한다(820단계). 재생시, 미디어의 특정 영역에 저장된 복호용 키를 이용해서 암호화 스트림을 복호화시킬 수 있다(830단계). 복호용 키는 여러번의 암호화 스트림에 대한 녹화가 이뤄질 때마다 해당하는 각각의 복호용 키가 저장될 수 있다. 이렇게 암호화된 스트림이 기록된 미디어의 내용을 다른 미디어나 장치로 복사할 경우, 데이터 기록영역에 기록된 비암호 스트림이나 암호 스트림 모두는 복사가 가능하지만, 상기 특정 영역에 저장된 복호용 키는 복사될 수 없다. 따라서 암호화된 스트림에 대해서는 다른 미디어등에서 복제가 불가능하게 된다.

본 발명에 의해 부가 유료 정보를 쉽게 배포 또는 방송하고 접근제어가 가능한 방송이나 미디어 전송(기록) 방식을 다음과 같이 제공할 수 있다. 암호 스트림은 추가로 요금이 지불되어야만 볼 수 있는 부가 정보로서 사용하고, 이들 암호 스트림을 해독하기 위한 복호용 키는 암호화되지 않은 이웃 스트림에 삽입된다. 수신자는 암호 스트림의 시청을 원할 경우 온라인이나 오프라인으로 비용을 지불하고 필요한 키나 카드, 비밀번호를 부여받으며, 이때 부여받은 값이 비암호 스트림을 해독할 복호용 키를 얻는데 필요한 값이 된다. 즉, 이중으로 암호화되어 있어서, 이 값이 없으면 비암호 스트림으로부터 복호용 키를 찾아내도 사용할 수 없도록 한다.

발명의 효과

본 발명에 의하면 선택적 데이터 스트림의 암호화 방식을 채용함으로써 다양한 비즈니스 모델에 유료 데이터를 안전하게 전송할 수 있고 억세스 되어 재생된 암호화 데이터에 대해 추가 복제를 방지할 수 있다.

(57) 청구의 범위

청구항 1.

영상 정보 전송 방법에 있어서,

비암호화 채널 데이터와 함께, 상기 영상 정보를 암호화한 채널 데이터를 다중 스트리밍 방식으로 전송하는 단계를 포함하고,

이때 상기 암호화된 채널의 스트림 데이터를 복호화하는데 필요한 키를 인접하는 비암호화된 채널의 스트림 데이터에 삽입하여 전송함을 특징으로 하는 영상 정보 전송 방법.

청구항 2.

제1항에 있어서,

상기 암호화 채널의 데이터 중 일부 스트림 데이터만이 암호화되어 전송됨을 특징으로 하는 영상 정보 전송 방법.

청구항 3.

제1항에 있어서,

상기 암호화 채널의 전체 스트림 데이터가 모두 암호화되어 전송됨을 특징으로 하는 영상 정보 전송 방법.

청구항 4.

암호화가 필요한 채널의 데이터를 전송하는 방법에 있어서,

암호화할 채널의 데이터 중 일부만을 암호화하여 소정의 스트리밍 방식으로 전송하는 단계를 포함하고,

이때 상기 암호화된 데이터를 복호화하기 위한 키를 상기 동일 채널의 스트림 데이터 중 암호화되지 않은 스트림내에 삽입하여 전송함을 특징으로 하는 영상 정보 전송 방법.

청구항 5.

암호화가 필요한 채널의 전송 및 수신 방법에 있어서,

암호화할 채널의 데이터 중 일부만을 암호화하여 소정의 스트리밍 방식으로 전송하고, 상기 암호화된 스트림을 복호화하기 위한 키를 암호화되지 않은 이웃 스트림에 삽입하여 전송하는 단계;

상기 이웃 스트림으로부터 상기 복호용키를 추출하는 단계; 및

상기 복호용 키를 사용하여 상기 암호화된 데이터 스트림을 복호화하여 재생하는 단계를 포함함을 특징으로 하는 암호화 채널의 전송 및 수신 방법.

청구항 6.

소정 전송 스트리밍 방식으로 전송된 암호화 데이터 스트림과 비암호화 데이터 스트림을 저장 매체에 기록(녹화)하여 재생하는 방법에 있어서,

전송된 데이터 스트림으로부터 암호화 스트림을 복호화하기 위한 키를 추출하여 상기 저장 매체의 소정 영역에 저장하는 단계;

전송된 암호화 스트림과 비암호화 스트림을 저장 미디어의 데이터 영역에 저장하는 단계; 및

상기 복호용 키를 이용하여 상기 암호화 스트림을 복호화하는 단계를 포함함을 특징으로 하는 암호화 데이터의 저장 및 재생 방법.

청구항 7.

제6항에 있어서, 상기 복호용 키가 저장되는 상기 저장매체의 소정 영역은

상기 암호화된 데이터 스트림이 외부로 복제되어 재생될 수 없도록 사용자 접근 및 저장 데이터이 외부로의 복제가 불가능한 영역임을 특징으로 하는 암호화 데이터의 저장 및 재생 방법.

청구항 8.

광고 콘텐츠와 사용자 이용 콘텐츠를 전송 및 수신하는 방법에 있어서,

상기 광고 콘텐츠는 암호화하지 않고 상기 사용자 이용 콘텐츠는 암호화하는 단계;

상기 광고 콘텐츠에 해당하는 스트림에 상기 암호화된 사용자 이용 콘텐츠를 복호화하는데 필요한 키를 삽입하는 단계;

상기 복호용 키가 삽입된 광고 콘텐츠를 상기 암호화된 사용자 이용 콘텐츠 앞에 위치시켜 전송하는 단계;

상기 광고 콘텐츠를 수신하여 시청하면 상기 복호용 키가 추출되어지는 단계; 및

상기 복호용 키를 이용하여 상기 사용자 이용 콘텐츠의 암호 데이터를 복호화하는 단계를 포함함을 특징으로 하는 콘텐츠 전송 및 수신 방법.

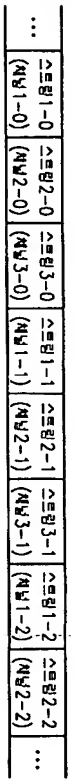
청구항 9.

제8항에 있어서,

상기 광고 콘텐츠를 사용자가 일정 시간 시청하도록, 상기 복호용 키는 상기 광고 콘텐츠의 소정 부분에 분산되어 들어 있음을 특징으로 하는 콘텐츠 전송 및 수신 방법.

도면

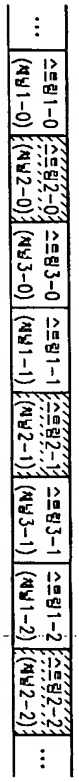
도면 1a


...
스트림1-0
(제1-0)
스트림2-0
(제2-0)
스트림3-0
(제3-0)
스트림1-1
(제1-1)
스트림2-1
(제2-1)
스트림3-1
(제3-1)
스트림1-2
(제1-2)
스트림2-2
(제2-2)
...

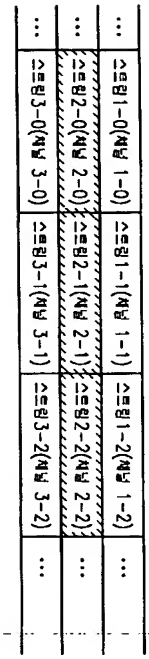
도면 1b


...
스트립1-0(채널 1-0)
스트립1-1(채널 1-1)
스트립1-2(채널 1-2)
...
...
스트립2-0(채널 2-0)
스트립2-1(채널 2-1)
스트립2-2(채널 2-2)
...
...
스트립3-0(채널 3-0)
스트립3-1(채널 3-1)
스트립3-2(채널 3-2)
...

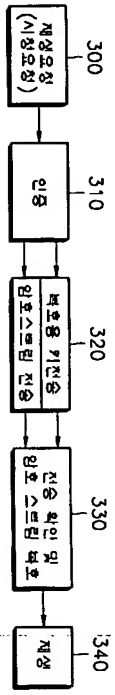
도면 2a


...
스큐1-0
(W1-0)
스큐2-0
(W2-0)
스큐3-0
(W3-0)
스큐1-1
(W1-1)
스큐2-1
(W2-1)
스큐3-1
(W3-1)
스큐1-2
(W1-2)
스큐2-2
(W2-2)
...

도면 2b

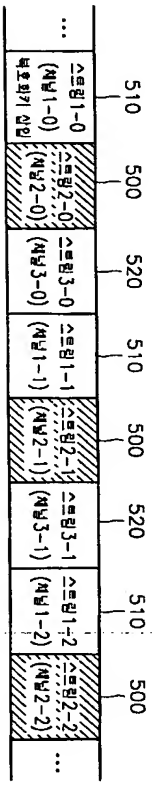

...
스트림1-0(채널 1-0)
스트림1-1(채널 1-1)
스트림1-2(채널 1-2)
...
스트림2-0(채널 2-0)
스트림2-1(채널 2-1)
스트림2-2(채널 2-2)
...
...
스트림3-0(채널 3-0)
스트림3-1(채널 3-1)
스트림3-2(채널 3-2)
...

도면 3

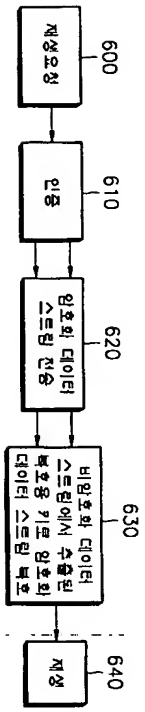

재생요청
(시청요청)
300
인증
310
복호용 키전송
암호스트림 전송
320
전송 확인 및
암호 스트림 복호
330
재생
340

도면 4

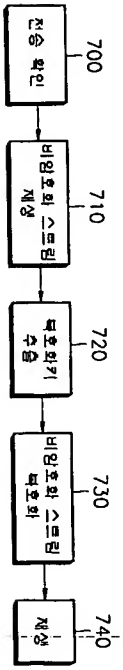
도면 5


...
스트림1-0 (채널1-0)
스트림2-0 (채널2-0)
스트림3-0 (채널3-0)
스트림1-1 (채널1-1)
스트림2-1 (채널2-1)
스트림3-1 (채널3-1)
스트림1-2 (채널1-2)
스트림2-2 (채널2-2)
...
510
500
520
510
500
520
510
500

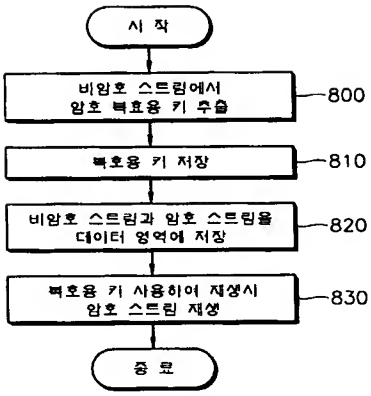
도면 6


재생요청
600
인증
610
암호화 데이터 스트림 전송
620
비암호화 데이터 스트림에서 수출된 복호용 키를 암호화 데이터 스트림 복호
630
재생
640

도면 7


전송 확인
700
비암호화 스트림 재생
710
복호화키 추출
720
비암호화 스트림 복호화
730
재생
740

도면 8


시 작
비암호 스트림에서 암호 복호용 키 추출
800
복호용 키 저장
810
비암호 스트림과 암호 스트림을 데이터 영역에 저장
820
복호용 키 사용하여 재생시 암호 스트림 재생
830
종 료